2024 디지털 보안 가이드

2024 디지털 보안 가이드

발행일 2024년 11월
글쓴이 변규홍
펴낸곳 진보네트워크센터
편집 다디잔
주소 03745 서울시 서대문구 독립문로8길 23 (천연동, 3층)
전화 02-774-4551
팩스 02-701-7104
홈페이지 https://guide.jinbo.net/digital-security-2024

2024 디지털 보안 가이드

들어가며

2015년 8월 진보네트워크센터와 정보인권연구소의 '디지털보안 가이드북 <국가감시로부터 자신을 보호하는 방법>' 발행 후 10년이 되어갑니다. 생성형 인공지능, 클라우드 협업 툴이 시민들의 일상, 시민사회단체의 업무에 스며들었습니다. 활동가들에게 스마트폰, 메신저, 협업 도구, 클라우드 등은 더 이상 낯설지 않습니다. 하지만 새로운 도구에 맞춰 꼭 알아야 할 디지털 보안 개념은 여전히 낯설고 어렵습니다.

2024년의 가이드는 2015년의 가이드 및 EEF(Electronic Frontier Foundation)의 SSD(Surveillance Self-Defence), Front Line Defenders의 Security in a Box 등의 가이드를 출발점으로 많은 내용을 재구성합니다. 디지털 보안 가이드를 미리 숙지하기 어려워도 최소한 이것만은 알아야 한다는 것을 체크리스트로 소개하고, 돌발 상황에 빠르게 대처할 방법을 단계적으로 찾을 수 있도록 배치하였습니다. 현재에 맞지 않는 내용은 과감히 덜어내고, 한국 시민사회단체에서 많이 사용되는 클라우드 협업 도구에 대한 내용과 '용어'에 대한 설명을 쉽고 빠르게 찾아볼 수 있도록 하는 데 초점을 맞추었습니다.
모든 사람이 똑같은 수준의 보안을 할 필요는 없습니다. 위협의 종류와 정도는 사람들마다 다릅니다. 그래서 적절한 보안을 위해서는 자신의 상황을 잘 파악할 필요가 있습니다. 보안에 대한 지식을 많이 갖고 있을수록, 자신에게 적합한 수준의 보안 조치를 취할 수 있을 것입니다. 이 가이드가 시민사회단체 활동가를 비롯한 디지털 보안을 원하는 모든 시민에게 도움이 되기를 바랍니다.

차례

0. 디지털 보안 가이드를 읽기 위한 가이드

0-1. 각 장에서 소개하는 내용

이 가이드를 소설책 읽듯이 읽어 나가기는 힘듭니다. 그래서 상황이나 요구에 따라 어떠한 부분을 먼저 읽으면 좋을지 정리했습니다. 물론 앞부분부터 읽으면서 하나하나 본인에게 필요한 보안 조치를 고민하는 것이 가장 좋습니다! 어떤 하나의 보안 조치를 취했다고 하더라도, 다른 곳이 취약하면 효과가 반감되기 때문입니다. 각 장을 다 읽기 어려울 땐, 각 장에서 어떤 내용을 꼭 숙지해야 하는지 돌아볼 만한 내용도 요약해 보았습니다. 단, 제안된 요약 내용을 절대 맹신하지 마세요.

0-1-1. 디지털 보안에 대한 이해

'디지털 보안에 대한 이해'는 특정한 보안 조치에 대한 것이 아니라, '디지털 보안' 전반에 대한 이해를 돕는 장입니다. 만 원 한 장을 지키기 위해 백만 원짜리 금고를 살 필요는 없습니다. 무조건 비싼 보안이 좋은 것은 아니라는 얘기죠. 온갖 보안 조치를 해도 비밀번호를 '1234'로 하면 의미가 없어집니다. 특정한 보안 조치에 대한 기술적인 이해가 아니라, 디지털 보안 자체에 대한 이해도 중요합니다. 가이드의 나머지 내용을 읽기 전에 꼭 한 번은 읽어주세요. 특히 <디지털 보안을 위한 7가지 원칙>, <디지털 보안 대책 마련하기>는 항상 숙지해주세요.

상황, 단계별로 필요한 챙길거리 모으기

- 기자에게 국회의원 스마트폰 화면 노출, ATM 줄 뒷 사람에게 비밀번호 노출과 마찬가지로 내 화면이 노출될 가능성을 충분히 고려하세요.
- 나(와 우리 단체) 말고 상대쪽에서 디지털 보안이 뚫리면 곤란합니다. 통신의 상대의 디지털 보안 수준도 함께 고민하세요.

적(!)의 능력을 과대/과소평가하지 말기

- 전국민의 모든 통신자료를 통신사, 빅테크 기업, 정부기관이 전부 실시간으로 감시하고 활용하는 일이 쉽지는 않다는 걸 유념하세요. 지레 겁먹지 않아도 됩니다.
- 하지만 중고등학생 정도만 되어도 가벼운 수준의 괴롭히기성 해킹, 랜섬웨어 등을 유포할 수 있습니다. 디지털 보안 공격 기술의 파괴력은 올라가고 난이도는 낮아지는 추세란 점을 잊지 마세요.

0-1-2. 비밀번호와 인증의 실제

비밀번호는 가장 많이 쓰이는 '인증' 수단이기 때문에, 대부분의 보안 조치에 쓰입니다. PC에 접근할 때, 이메일 계정에 접근할 때, 은행 거래를 위해, 보안 통신을 위해, 이 작업을 하는 사람이 나 자신이라는 것을 '인증'해야 하는 여러 곳에서 비밀번호가 사용됩니다. 워낙 많은 곳에서 비밀번호가 사용되니 기억하기 쉬운 것을 사용하거나, 같은 비밀번호를 여러 곳에서 사용합니다. 보안의 가장 큰 취약점 중의 하나입니다. 2장에서는 비밀번호, 2단계 인증(2FA)을 비롯한 다양한 인증방법을 소개하고, 특히 비밀번호를 어떻게 만들고, 어떻게 관리해야 하는지에 대해 소개하겠습니다.

핵심 어려운 비밀번호, 비밀번호 관리 도구, 2단계 인증, 패스키

- 길고, 나만 외울 수 있고, 타인은 상상도 못 할 비밀번호, 비밀번호 관리자, 2단계 인증, 패스키. 모르는 말이 없도록 하세요.

KeePassXC, KeePassDX, StrongBox 등의 '비밀번호 관리 도구' 쓰기

- 비밀번호를 좀더 안전하게 사용하려면 '비밀번호 관리 도구'를 사용해보세요. 가급적 계정마다 서로 다른 비밀번호를 쓰기 위해서라도 비밀번호 관리 도구는 선택이 아닌 필수입니다. '비밀번호 관리 도구' 자체의 비밀번호는 외우기 쉽지만 매우

어렵게 설정하고, 각 계정의 비밀번호 입력은 '비밀번호 관리 도구'에게 맡기세요.

TOTP등의 2단계 인증, 패스키 등의 인증 방식 사용하기

- 비밀번호 인증만으로는 보안 위협을 막기 어렵습니다. '2단계 인증'을 쓸 수 있는 경우에는 최대한 2단계 인증을 쓰세요. 특히 휴대전화 등의 기계를 분실할 일이 없다면 패스키(Passkey) 같은 인증방식이 훨씬 안전합니다. 패스키가 설정된 기계를 분실했어도 당황하지 말고 해당 패스키를 폐기할 방법만 찾으면 됩니다.

0-1-3. 악성 코드와 해킹에 대한 이해

누구나 바이러스에 걸려본 경험이 있을 것입니다. 자칫 소중한 자료를 날릴 수도 있습니다. 특히나 해커나 범죄자만 바이러스와 같은 악성 소프트웨어를 만드는 것이 아닙니다. 스파이웨어를 통해 정보기관이 합법적으로 온라인 감시를 하고 있는 나라들도 있습니다. 비록 모든 악성 소프트웨어를 막을 수는 없을지라도, 컴퓨터를 사용하고 있는 이상 이에 대한 대비는 필수입니다. 악성 코드, 해킹, 바이러스 등 여러 가지 개념들에 대해 "이런 것도 해킹이었어?" 하고 놀랄 수 있는 지점들을 소개합니다.

넓은 의미의 해킹 이해하기

- 허락해준 적 없는 일을 하는 것 대부분을 넓은 의미의 해킹이라고 봐도 됩니다. 허락한 적 없는 파일이나 대화 내용에 접근하는 것 자체도 넓은 의미의 해킹에 포함됩니다. 내가 언제 어떤 웹 사이트를 방문했는지를 알아내거나, 내 계정의 비밀번호를 바꿔 버리거나, 내 계정의 비밀번호를 알아내거나, 내 이메일 중 일부를 몰래 지워버리거나, 내 계정으로 몰래 댓글을 쓰거나, 내 데이터 일부를 지워 버리거나. 넓은 의미의 해킹이 어떤 뜻을 갖는지 명심하세요.

0-1-4. 파일과 기기, 운영체제의 보안

노동, 인권 단체의 사무실이 수사 기관에 의해 압수수색을 당하는 일은 드물지 않게 발생합니다. 활동가의 사무실 컴퓨터나 집에 있는 컴퓨터 역시 마찬가지입니다. 압수된 저장장치의 데이터는 '포렌식 기술'에 의해 분석됩니다. 이렇게 추출된 정보들은 활동가를 기소하거나, 혹은 일상적으로 '사찰'하기 위해 사용될 수 있습니다. 자신과 단체의 소중한 자료가 유출되는 것을 막기 위해서는 우선 보안이 필요한 데이터를 암호화해야 합니다. 이러한 데이터에 접근할 수 있는 기기의 보안도 신경써야 합니다.

경우에 따라 데이터를 안전하게 영구 삭제해야 할 경우도 있습니다. 2012년 대통령 선거 기간 중 댓글 여론 조작을 했던 국가정보원과 이들의 범행을 은폐하려고 했던 서울지방경찰청 역시 증거를 없애기 위해 영구 삭제 프로그램을 사용한 것으로 알려졌습니다. 하지만 2024년 현재는 이러한 방법을 쓰기 어렵습니다. 데이터를 안전하게 삭제하기 어려운 이유를 소개하고, 몇 가지 방법을 제안합니다.

요새 집회나 시위를 하다가 연행이 되었을 때, 휴대전화를 압수수색하는 경우가 많아지고 있습니다. 휴대전화에는 우리가 주고받은 문자 메시지, 메신저 내용, 통화 내역, 사진, 검색 기록 등 매우 민감한 개인정보가 저장되어 있습니다. 미리 미리 휴대전화 압수수색에 대비해야겠죠. 휴대전화 역시 데이터를 암호화하거나 안전하게 관리할 방법이 있는지 살펴야 합니다.

VeraCrypt, BitLocker(윈도우 장치 암호화), FileVault 등의 '볼륨 암호화' 도구로 디스크 암호화하기

- 데이터가 들어있는 기기를 뺏기는 것만으로 그 속에 있는 정보도 뺏긴다면 곤란합니다. VeraCrypt, BitLocker(윈도우 장치 암호화), FileVault(맥) 등을 쓰면 '비밀번호' 없이는 기기 속 파일에 접근할 수 없습니다. 파일 자체가 암호화된 형태로 저장되어 있는 상황을 유지하세요.

아이폰의 '차단 모드'(Lockdown Mode), 갤럭시 스마트폰의 '최대 제한 기능' 사용

- 스미싱 공격 집중 등 내 스마트폰을 노린 실질적인 보안 위협이 실시간으로 진행중일 때, 아이폰의 '차단 모드'(Lockdown Mode), 갤럭시 스마트폰의 '최대 제한 기능' 사용을 고려하세요. 스마트폰의 여러 기능이 멈추지만, 그만큼 좀더 안전해집니다.

0-1-5. 통신, 이메일 및 메신저 보안

지난 2014년, 세월호 집회를 주도했다는 이유로 전 노동당 부대표 정진우씨의 카카오톡 메시지 내용이 압수수색된 사실이 알려졌습니다. 개인들 간의 사적인 통신 역시 국가 기관의 사찰로부터 안전하지 않다는 사실이 알려지면서 사이버 망명 바람이 일기도 했습니다. 카카오톡 뿐만이 아니라, 인터넷 이용 전체를 감청하는 '패킷 감청'도 가능합니다.

감청 당하지 않기 위해서는 인터넷을 통해 소통할 때 '암호화'를 해야 합니다. 카카오톡도 논란 이후, '종단간 암호화', 즉 통신 당사자 사이의 모든 구간에서 암호화 통신을 제공하는 프라이버시 모드를 도입하였습니다. 음성 전화, 문자 메시지, 메신저, 이메일 등을 통해서 소통을 할 때 암호화된 통신을 할 수 있는 방법을 살펴봅시다. 스마트폰이나 PC에서 사용하는 메신저, 이메일 등을 어떻게 암호화할 수 있는지, 과거부터 쓰이던 기법부터 요즘의 방법까지 다뤄봅니다.

모든 통신은 서로 대화를 주고받는 2명 이상이 존재합니다. 따라서 혼자서 이 프로그램들을 설치해서는 의미가 없겠죠. 해당 프로그램을 통해서 통신할 수 있는 사람들이 많아져야 프로그램의 유용성이 증가할 것입니다. 카카오톡으로부터 벗어나기 힘든 이유도 자신과 메시지를 주고받는 사람들이 이미 그 안에 많이 존재하기 때문이죠.

한국 사회 운동 내에서는 텔레그램이 많이 사용되고 있기도 합니다. 어떤 프로그램을 쓰더라도, 그 프로그램이 어떤 보안성을 제공하는지 잘 따져보고, 소통을 하고자 하는 공동체 내에서 적절한 프로그램을 선택해야 할 것입니다. 시그널(Signal)이 주목받는 이유와 함께 좀더 안전하게 시그널 메신저를 쓰는 방법도 소개합니다.

핵심 **정말로 '암호화'된 통신이 믿을 수 있게 보장되는지 알기**

- 인터넷으로 주고받는 정보는 휴대전화 기지국, 통신사 등을 거치는 과정에서도 안전하게 보호되어야 합니다. '종단간 암호화', '공개키 암호화'같은 표현에 익숙해지세요.

시그널 등의 '종단간 암호화' 메신저 쓰기

- 보안이 중요한 대화는 시그널 등의 '종단간 암호화' 메신저를 사용하세요. 어떤 메신저를 사용하더라도 '종단간 암호화'가 정말 적용되어 있는지 확인하세요. '링크 미리보기'등의 기능을 끄세요. 메신저의 '메시지 전달' 기능이 다른 사용자의 신원을 노출하지 않게 꼭 유의하세요. 보안이 필요한 대화는 자동 삭제되게 설정하세요. '알림창'에 메시지가 뜨지 않게 설정하세요.

0-1-6. SNS, 홈페이지 보안

보안만을 생각한다면 트위터, 페이스북 등 소셜 네트워크를 사용하지 않는 것이 좋습니다. 소셜 네트워크 서비스는 기본적으로 나의 사회적 관계망을 활용하는 서비스이기에, 최소한 '나의 사회적 관계'를 드러내기 때문입니다. 또한 사용하다 보면 내 위치, 관심사, 취향 등도 드러내기 십상입니다. 그러나 현실적으로 많은 사회 운동의 활동가들이 소셜 네트워크 서비스를 사용하고 있고, 자신의 활동을 알리고 대중과 소통하는 공간이기도 합니다. 소셜 네트워크 서비스를 이용해야 한다면, 불필요하게 자신을

드러내지 않도록 보안 설정을 하는 방법을 익혀둘 필요가 있습니다.

또한 우리 단체가 직접 홈페이지를 운영하는데 우리 단체의 홈페이지를 통해 악성 코드가 유포되거나 단체 내의 개인정보가 유출된다면 큰 문제가 되겠습니다. 이러한 문제를 사전에 예방하기 위해 단체 홈페이지에 최소한으로 챙겨야 하는 보안 요소들에 대해서도 소개합니다.

핵심 **정보의 공개 범위 확인하기**

- 나 혹은 내가 속한 단체의 SNS 계정이나 홈페이지가 악성 코드를 전파하는 장소가 되면 곤란합니다. 또, 내가 원치 않는 정보가 공개되어 있어도 곤란합니다. 정보의 공개 범위를 확인하고, 검색 엔진에 노출된 범위를 확인하세요.

0-1-7. 클라우드 서비스 및 협업 툴 보안

구글 독스(Google Docs), 노션(Notion)등 다양한 클라우드 서비스 및 협업 툴이 시민사회단체의 업무 전반에 걸쳐 사용되고 있습니다. 하지만 이러한 협업 툴의 구체적인 보안 설정에 대해 둔감한 경우가 많습니다. 구체적으로 어떤 지점들에 유의해야 하는지를 소개합니다. 특히 2023년부터 다종다양한 생성형 AI 서비스에 의한 새로운 디지털 보안 문제들이 나오고 있습니다. 이러한 문제들에 대응하는 방법도 소개합니다.

'활성 세션'을 모니터링하면서 이상 징후 발견시 '활성 세션' 종료하기

- 나 자신을 포함한 누군가가 언제, 어디서 로그인 상태를 유지하고 있는지 모니터링하세요. '활성 세션' 검사를 정기적으로 진행하세요.

클라우드로 자료를 공유할 땐 '주소를 아는 누구나' 접근하지는 못하게 제한하기

- 구글 드라이브, 드롭박스 등을 사용하여 파일을 공유할 때 '링크가 있는 사람

누구나' 편집할 수 있는 권한을 부여하지 마세요. 편집이 필요한 사람 모두가 계정이 있는 협업 툴을 사용하고, 계정 목록을 취합해 접근 권한을 관리하세요.

각종 AI 서비스의 편의성과 위험성 맞교환 확인하기

- 번역, 녹취 풀이 등 다양한 분야에서 AI 기술 기반 서비스들이 어떤 이용약관으로 어떤 정보를 수집하는지 확인하세요. 이용약관을 믿을 수 있다면 최소한 이용약관이 지켜질 때 어떤 정보가 노출될 수 있는지 위험성을 숙지하고 사용하세요.

0-1-8. 사무실, 물리적 보안 및 비대면 환경 보안

2024년 언론보도에서는 대법원 등 주요 국가기관에서 '인터넷 공유기'에 해당되는 기기가 해킹되어 수 년간 해외로 정보가 유출되었다는 내용이 다뤄졌습니다. 단체 사무실의 인터넷 공유기도 디지털 보안의 약한 고리가 될 수 있습니다. 특히 물리적인 영역에서의 보안 조치가 필요합니다.

핵심 공유기 관리, 참석자 확인 방법

- 사무실의 인터넷 공유기에 올바른 관리자 비밀번호가 설정되어 있는지, 제3자가 인터넷 공유기 등을 건드릴 수는 없는지 확인하세요. 화상회의의 참석자가 별도로 녹음을 하거나 촬영을 할 가능성을 염두에 두세요. 화상회의의 참석자가 실제 참석자가 맞는지 확인할 방법을 마련하세요.

0-1-9. 이미 벌어진 보안 사고 대처하기

휴대전화, 특히 스마트폰은 유용한 도구이지만, 나를 감시하는 최적의 도구가 될 수도 있습니다. 내 위치가 항상 드러나기 때문에, 내가 집회에 참석한 증거로 사용될 수도 있고, 휴대전화를 통해 내 위치를 추적할 수도 있습니다. 휴대전화 실시간 위치추적과 기지국 수사 등은 한국의

수사 기관도 많이 사용하는 기법입니다. 집회에서 연행이라도 되면 휴대전화를 압수당하기도 합니다. 분실한 휴대전화의 비밀번호나 패턴이 너무 단순하면 제3자가 휴대전화 속 내용을 열어볼 수도 있습니다. 휴대전화 보안에 각별히 신경 써야 하는 이유입니다. 하지만 이러한 상황에 놓이기 전까지는 사전에 대비하기 쉽지 않습니다. 사후적으로 보안 사고에 어떻게 대처해야 하는지를 다뤄봅니다.

핵심 **분실한 기기에 연결된 계정 비활성화하기**

- 흔히 벌어질 수 있는 보안 사고에 대비하기 위해 <파일과 기기, 운영체제의 보안> 장에서 설명하는 내용 중 꼭 챙겨야 하는 내용을 챙기지 못했더라도, 최소한으로 취할 수 있는 <계정 비활성화> 등 사후적인 조치들을 숙지하세요.

부록. 보안 위협 평가 체크리스트 (안)

디지털 보안 가이드를 읽고 우리 조직에 적용하기 위한 체크리스트를 우리 조직 스스로 만들어야 합니다. 참고가 될 만한 체크리스트를 제안합니다.

부록. 디지털 보안 참고자료

디지털 보안 가이드에서 참고한 국내외 디지털 보안 관련 참고자료를 소개합니다.

1. 디지털 보안에 대한 이해

우리는 일상에서 온갖 디지털 기기를 사용하면서 살아갑니다. 스마트폰, 컴퓨터, 노트북, PC를 비롯한 여러 전자기기를 씁니다. 이러한 디지털 기기를 이용해 우리는 정보를 관리하고, 다른 사람과 주고받습니다. 여러 상황 속에서 이러한 정보들이 제3자에게 노출된다면 그 자체로도 심각한 문제일 것입니다. 내가 주고받은 이메일을 볼 수 있는 사람은 오직 나 자신뿐이어야 합니다. 우리 단체가 외부 단체와 주고받은 메시지를 볼 수 있는 사람도 오직 우리 단체의 사람뿐이어야만 합니다.

디지털 보안의 핵심은, 디지털 기기를 사용하여 일어나는 다양한 활동과 정보처리를 오직 그럴 권한이 있는 사람만 할 수 있도록 하는 데 있습니다. 반대로 권한이 없는 사람이 그러한 행위를 했다면 이를 빠르게 알아차리고 이에 대응하는 것도 그만큼 중요합니다. 사전에 디지털 보안을 위해 어떤 준비를 했느냐에 따라 대응할 수 있는 위협과 대응할 수 없는 위협이 달라지고, 피해를 어디까지 줄일 수 있는지도 달라집니다.

기술은 끊임없이 진보하고, 지키려는 자와 뚫으려는 자의 창과 방패의 싸움도 계속됩니다. 디지털 보안 가이드를 통해 새롭게 등장하는 위협들을 알아보고, 특별히 좀더 신경써야 하는 지점들을 놓치지 않도록 해 봅시다.

1-1. 디지털 보안이란?

보안(保安)은 비밀 따위가 누설되지 않게 보호한다는 뜻입니다.[1]
디지털 보안은 특히 디지털 시대에 비밀 따위가 누설되지 않게
보호하는 것을 뜻합니다. 여기에는 사생활이나 개인정보를
비롯한 각종 정보나 자료, 개인이나 단체의 명의, 어떠한 행동을
하거나 하지 않았음에 대한 증명 등이 포함됩니다.

많은 경우 디지털 보안은 해킹과 연결되어 설명되곤 합니다. 디지털 보안에서
해킹은 악의를 가진, 권한이 없는 사람이 보안 대상인 정보를 취득하거나
위, 변조하는 일을 말합니다. 여기에는 단순히 컴퓨터나 스마트폰을
고장내는 일, 데이터를 지워버리는 일, 유출한 데이터를 빌미로 협박하는
일 등 다양한 단계가 파생됩니다. 물론 좁은 의미의 해킹과 구분하여
피싱 사기 사이트 운영, 파밍 사기 등을 논하기도 합니다. 또한 디지털
보안은 국가기관 혹은 각종 기업 등의 사찰, 검열에 대한 저항을 뜻하기도
합니다. 내가 혹은 우리 단체가 인터넷, 디지털 기기를 사용하여 언제
무엇을 했는지에 대해 감시받지 않을 자유를 누릴 수 있어야 합니다.

위협이란 무엇인지, 전에 없었던 디지털 보안 위협은 무엇이 있는지,
어떤 원칙들을 알아야 하는지, 그래도 일단 애매하다면 예를 들어
어떤 판단을 참고할 수 있는지를 하나씩 차근차근 살펴보겠습니다.

1-1-1. 사례: 화상회의 참가자 모두가 딥페이크

영국계 건축회사 에이럽(ARUP) 홍콩지사는 제2롯데월드타워를 설계하는

1 https://dic.daum.net/word/view.do?wordid=kkw000112484&supid=kku000139808

등 여러 가지로 한국과 인연이 있는 회사입니다.[2] 2024년 2월, 에이럽 홍콩지사에서는 영화 속에서나 볼 수 있을 법한 디지털 보안 사고가 일어났습니다. 회사의 재무 책임자(CFO)에게서 돈을 송금하라는 연락을 받고, 이어서 참석한 화상 회의에서 돈을 송금하라는 동료 직원들의 말을 들은 회계 담당자가 340억의 돈을 사기당한 사건입니다.[3] [4] 알고 보니 화상회의에 참석한 직원들의 얼굴 모습과 목소리 모두 가짜였습니다. 딥페이크(Deepfake)라는 기술에 속아 당한 것입니다.

'보이스피싱', '전기통신금융사기' 피해자가 속출하고 있는 2024년, 시민들의 휴대폰에는 카카오톡, 문자 등 온갖 방법으로 사칭 연락이 찾아옵니다. 가까운 가족이나 친구, 동료 활동가를 사칭하면서, 지금 휴대폰을 잃어버려서 전화를 할 수 없는데 급한 상황이니, 지금 즉시 이 계좌번호로 돈을 송금해 달라는 이야기를 하면 의심부터 해야 하는 시대입니다. 하지만 만일 이런 연락이 메시지가 아닌 전화로, 심지어 영상통화로, 무려 여러 사람이 동시에 참여하는 화상회의의 형태로 온다면 속지 않을 수 있을까요?

물론 방법은 있습니다. 영상통화나 화상회의에서 눈에 보이는 영상, 소리뿐만 아니라 그들의 계정 정보를 확인하고, 별도의 채널로 참석자들의 신원을 확인하는 것입니다. 다소 불편하고 자칫 요식행위가 될 수도 있지만 시대가 변화하고 코로나19 등의 이유로 비대면 업무가 보편화되면서, 특히 생성형 AI 기반의 위협이 다가오면서 그렇게 되었습니다.

물론 여전히 어떤 위협은 과대평가되어 있고, 어떤 위협은 과소평가되어 있습니다. 디지털 보안 가이드와 함께 그 적절한 균형을 찾아봅시다.

---

2 https://imnews.imbc.com/news/2015/econo/article/3645127_31251.html
3 https://www.khan.co.kr/world/world-general/article/202402051422001
4 https://www.sedaily.com/NewsView/2D98HW52A6

1-1-2. 디지털 보안을 위한 7가지 원칙

디지털 보안을 위해 반드시 알아야 하는 7가지 원칙을 소개합니다.
가이드의 나머지 내용을 읽을 때 항상 염두에 두어 주세요.

아는 만큼 지킬 수 있다

디지털 보안에서 가장 중요한 것은 '아는' 것입니다. 다른 그
무엇보다도 자신이 처한 상황을 정확히 알고, 이에 대한 대책을
세우기 위해 무엇을 아는 것이 필요한지 알아야 합니다.
어떤 정보를, 누가 왜 노리고 있는지, 얼마나 심각하고 일어남직한
위기인지, 이를 지키기 위해 누구를 믿을 수 있는지, 얼만큼의
노력을 투입할 수 있는지 알고 있나요? 최근 주변에서 발생하고
있는 디지털 보안 침해사고는 어떤 것이 있는지 알고 있나요?
이러한 질문에 대한 답변을 통해 자신의 디지털 보안
요구사항을 더 잘 평가하고, 적절한 보안 계획 또는 위협 모델을
수립할 수 있습니다. 이 과정에서 여러분은 생각보다 더 많은
통제력을 가지고 있다는 것을 깨달을 수 있습니다.

전체 과정에서 가장 취약한 지점을 찾아라

현재 디지털 보안의 취약 수준은 전체 시스템 중 가장 취약한 부분에
의해 결정됩니다. "쇠사슬의 강도는 가장 약한 고리에 달려있다"라는
격언처럼, 보안 시스템의 안전성도 가장 취약한 요소에 의해 결정됩니다.
집의 보안을 예로 들면, 현관문에 최신형 도어록(잠금장치)을 설치했어도
창문이 열려 있다면 도둑이 집으로 침입할 수 있겠습니다. 어디가 가장
튼튼한지보다, 어디가 가장 연약한지가 중요하다는 말입니다. 최신 보안
메신저를 써서 복잡한 암호화를 적용한 채 정보를 주고받았어도, 정작
메시지를 사진으로 찍어서 암호화 없이 스마트폰에 저장해 둔다면?

이메일을 암호화하여 주고받았지만 정작 이메일을 마지막으로 열어본 노트북에는 암호화되지 않은 상태로 저장되어 있다면? 기기 도난 시 정보 유출의 위험이 있습니다. 또한 '나'의 디지털 보안이 아무리 철저해도 '나'와 정보를 주고받는 상대방의 디지털 보안이 취약하다면 상대방의 실수로 정보가 유출되는 것을 막을 수 없습니다.
결국, 디지털 보안은 전체 과정에서 가장 취약한 지점을 지속적으로 찾아 단계적으로 보완해 나가는 작업임을 명심해야 합니다.

단순할수록 안전하고 쉬워진다

디지털 보안을 위한 실천은 일상에서 혹은 통상적인 업무 과정 전반에서 언제나 실행할 수 있어야 합니다. 최신 소프트웨어 수십 가지와 복잡한 규칙을 사용하는 것보다, 앞선 원칙에서 이야기한 '가장 취약한 요소'를 찾고 보완하는 것이 훨씬 중요합니다. 디지털 보안 절차가 너무 복잡해지면 '전체 과정'의 구조, 즉 시스템이 복잡해져서 가장 취약한 요소가 무엇인지 찾기 어려워질 수 있습니다. 또 복잡성 때문에 절차를 생략하는 잘못된 습관이 들 수도 있습니다. 따라서 디지털 보안 대책은 가급적 단순하고 쉽게 유지하세요.

더 비싸다고 더 안전한 것은 아니다

디지털 보안에 대한 가장 큰 오해 중 하나는 값비싼 보안 대책이 더 높은 보안을 제공한다는 것입니다. 실제로 FBI에서 이런 심리를 노리고 광범위한 사찰을 위해 값비싼 보안 스마트폰을 판매했던 사례가 있습니다.[5] 단순히 값이 비싸다, 업계에서 유명하다는 이유로 더 높은 보안 수준을 제공한다고 생각하지 않도록 유의하세요. 오히려 "종이에 인쇄한 디지털 정보는 반드시

5 https://www.npr.org/2024/06/04/nx-s1-4987090/planet-money-how-the-fbis-fake-cell-phone-company-put-criminals-into-jail-cells
https://en.wikipedia.org/wiki/Operation_Trojan_Shield

회의 직후 파쇄기에 넣는다"같은 보안 대책이 나올 수도 있습니다.

현 시점에 누구를 얼만큼 믿을지 판단하라

현재 디지털 보안 업계에서는 제로 트러스트(Zero Trust) 원칙을 이야기합니다. 이 말은 일견 자기 자신 이외에 누구도 믿지 말라는 것처럼 오해되곤 합니다. 하지만 실제로는 제로 트러스트 원칙은 그런 뜻이 아닙니다. 예를 들어 우리의 일상 속에서 우리는 가족, 동료, 지인 중 전문가의 의견을 신뢰하지요. 법적인 문제가 생기면 변호사에게 중요한 비밀을 털어놓기도 합니다. 물론 변호사들이 그 비밀을 누설할 가능성이 없지 않지만, 그렇기 때문에 우리는 상황에 따라 얼만큼의 믿음을 얼마간의 시간동안 가질지를 항상 판단합니다. 클라우드 협업 툴을 예로 들면, 드롭박스나 구글드라이브에 올려둔 문서는 편리하게 접근할 수 있다는 장점이 있지만, 드롭박스나 구글에서 그 문서에 접근할 가능성이 있다고 판단할 수도 있습니다. 따라서 이들을 얼만큼 믿을지를 항상 판단해야 합니다. 오늘 믿을 만한 보안 대책도 다음 달에는 믿지 못할 이유가 생길 수 있습니다.

완벽한 보안은 없고, 언제나 타협점이 있음을 명심하라

한 차례 디지털 보안 대책을 수립했다고 해서 완벽한 철통 보안이 완성된다고 생각하면 안 됩니다. 또한 많은 경우 디지털 보안 대책은 일정 수준 이상의 불편함을 감수하는 타협을 필요로 합니다. 이러한 타협은 나 자신, 우리 조직에서 전반적으로 이뤄져야 합니다. 이론상 완벽해 보이는 보안 정책도, <단순할수록 안전하고 쉬워진다> 원칙에서 이야기했듯 지키지 않는 버릇이 들면 바로 문제가 됩니다. 또한 디지털로 연결된 상대방의 모든 행동을 통제할 수 없다는 것도 주의해야 합니다. 상대방에게 우리의 보안 대책을 따를 것을 강제할 수

없다면, 이로 인해 어떤 위험이 생길 수 있는지는 통제 불가능한 타협의 지점으로 인식하고 디지털 보안 대책 수립 시 참고해야 합니다.

오늘 안전했다고 내일도 안전한 것은 아니다

디지털 보안 대책을 수립하는 과정은 한 번 하고 끝나서는 안 됩니다. 시간이 흐르면서, 과거 안전했던 것으로 알려진 방식들에 숨어있던 보안 취약점이 뒤늦게 발견되곤 합니다. 오늘 한 차례 보안 대책을 수립했다는 것에서 멈추지 말고, 시간이 흐르면 계속 재평가하도록 합시다.

1-1-3. 디지털 보안 대책 마련하기

모든 종류의 위협을 차단할 수 있는 마법같은 디지털 보안 대책은 없습니다. 특정한 도구를 사용하는 것 자체가 중요한 것이 아니라, 어떤 위협이 실존하는 위협인지, 얼마나 심각한 위협인지, 어떻게 대응하여 피해를 최소화할 것인지가 중요하기 때문입니다. 개인마다, 조직마다 상황이 다르기 때문에 각 개인 혹은 단체가 직접 자신만의 혹은 우리만의 '디지털 보안 대책'을 마련해야 합니다. 디지털 보안 대책을 마련하기 위한 과정을 '위협 모델링'이라고 부르기도 합니다.

또한 디지털 보안 위협은 새로운 기술의 도입 혹은 발전에 따라 나날이 달라지기 때문에, 디지털 보안 대책은 한 번 마련하고 끝날 것이 아니라 정기적으로 점검하고 개선해 나가야 합니다. '지켜야 할 대상' 자체가 변화할 수도 있고, 이를 노리는 상대도 달라질 수 있기 때문입니다. 디지털 보안 대책을 마련하기 위해 아래와 같은 6가지 질문을 던져봅시다.

- 디지털 보안으로 보호할 대상은?
- 보호할 대상을 노리는 상대는?

- 위협에 따른 예상 피해의 수준은?
- 실제로 위협이 일어날 가능성은?
- 감당 가능한 불편, 투입할 자원의 규모는?
- 현 시점의 '우리 편'과 의논할 사항은?

디지털 보안으로 보호할 대상은?

디지털 보안 대책 마련의 시작은 무엇을 지키고자 하는지를 구체화하는 데서 출발합니다. 디지털 보안의 관점에서는 디지털 기기를 사용하여 오고 가는 '정보'가 주된 보호 대상이 됩니다. 그 중에서도 어떤 정보를 보호하고자 하는지 구체화할수록 좋습니다. 이메일, 메신저 대화 내용, 주소록의 연락처, 사진, 스크린샷, 문서, 파일 등 다양한 형태의 정보가 있습니다.

정보의 내용 자체가 유출 등의 형태로 알려지지 않게 보호해야 하는지, 아니면 정보의 내용이 제3자에 의해 위조나 변조되지 않는 것이 중요한지도 살펴야 합니다. 단체의 공식 홈페이지에 올라오는 공지, 입장문 등을 단체의 외부인이 게시할 수 있어서는 안 됩니다. 조직의 업무용 PC에 있는 지난 수 년간의 업무 파일이 갑자기 훼손되어도 곤란합니다.

정보가 저장되어 있는 기기, 정보에 접근할 수 있는 권한이 있는 계정 등 디지털 보안으로 보호해야 할 대상은 정보와 관련된 여러 가지 대상으로 확대될 수 있습니다.

> 지키고자 하는 정보가 무엇인지, 어디에 저장되어 있는지, 누가 접근할 수 있는지, 다른 사람들이 접근하지 못하게 하는 현재의 방법은 무엇인지 정리해 봅시다.

보호할 대상을 노리는 상대는?

지켜야 할 대상이 구체화되면, 어떤 상대가 이 대상을 노리는지, 어떤 상대로부터 이 대상을 지켜야 하는지 알아야 합니다. 간단히, 과장하여 말하면 '적'이 되겠습니다. 지켜야 할 정보, 디지털 보안을 위협하는 적이 누구인지는 천차만별로 다릅니다. 대체로 이 정보를 손에 넣으면, 혹은 이 정보를 파괴하면 이익을 얻는 존재를 찾으면 됩니다.

직장의 상사, 경쟁자, 정부 기관, 해커 등 다양한 적이 정보를 노릴 수 있습니다. 너무 범위를 넓히지 않기 위해서는 대상과 상대의 연관성을 잘 분석하는 것이 중요합니다.

> 이미 알고 있는 상대, 혹은 여러 가지 이유로 보호할 대상을 노릴 만한 상대가 누구인지 정리해 봅시다. 특정 개인, 정부 기관, 특정 기업일 수 있겠습니다.

위협에 따른 예상 피해의 수준은?

지켜야 하는 정보를 지키지 못했을 때 얼마나 큰 피해가 발생하는지를 판단하는 것은 디지털 보안 대책을 마련할 때 매우 중요한 요소입니다. 보호할 대상을 노리는 상대가, 그 상대로부터 지키고자 했던 정보를 성공적으로 손에 넣으면 이로 인해 구체적으로 어떤 피해가 일어나는지를 알아야 합니다.

이를테면, '적'은 이 정보를 이용해 협박을 해올 수도 있습니다. 혹은 '적'은 삭제되면 안 되는 정보를 삭제할 수도 있습니다. 그런 일이 실제로 일어났을 때 얼마나 큰 곤경에 처하는지를 명확히 알아야 합니다. 어떤 위협은 사실 큰 피해를 초래하지 않을 수도 있지만, 어떤 위협은 나 자신 혹은 우리 단체에 치명적인 피해를 입힐 수도 있습니다.

> 지키고자 하는 정보에 성공적으로 접근한 '적'이 이를 이용하여 취할만한 행동들을 정리해 봅시다. 금전적인 이익을 얻으려 하여 이로 인한 피해가 발생할 것인지 등을 알 수 있습니다.

실제로 위협이 일어날 가능성은?

'위험'(Risk)은 보호 대상에 대해 특정한 위협이 실제로 발생할 가능성을 말합니다. 보호할 대상을 노리는 상대의 능력과 의지에 큰 영향을 받습니다. 예를 들어 이동통신사를 생각해 봅시다. 극단적인 가정에서 이동통신사는 우리의 모든 데이터에 접근할 능력이 있지만, 이동통신사가 직접 인터넷에 나 혹은 우리 조직의 명예를 훼손하기 위해 사적 정보를 올릴 위험성은 어떨까요? 이는 '위협'과 '위험'을 구분하는 것이 매우 중요하다는 것을 시사합니다.

일어날 수 있는 일 그 자체를 일컫는 것이 '위협'이라면, 그런 일이 정말로 일어날 가능성을 따지는 것이 '위험'입니다. 위험은 개인마다, 조직마다, 시기와 주변 여건의 변화에 따라 크게 달라질 수 있다는 점에 유의해야 합니다.

어떤 위협은 무섭지만 실제로 일어날 가능성이 매우 희박하고, 또 어떤 위험은 엄청나게 자주 일어나지는 않지만 치명적일 수 있습니다. 디지털 보안 대책을 마련함에 있어 위험에 대한 판단은 매우 주관적이며, 따라서 각자 자신만의 위험 판단 기준을 갖고 있어야 합니다.

> 진지하게 대응 방법을 고민해야 하는 위협을 정리해 봅시다. 이 과정에서 일어날 가능성이 희박하여 무시해도 되는 위협, 혹은 별다른 피해가 예상되지 않는 위협을 나눠 봅시다.

감당 가능한 불편, 투입할 자원의 규모는?

클라우드 협업 툴, 생성형 AI를 비롯한 디지털 기술의 발전은 다양한 업무 편의와 효율성을 가져오고 있지만, 그만큼 새로운 형태의 디지털 보안 위협을 가져오고 있습니다. 높은 수준의 디지털 보안을 위해선 그 무엇보다 평상시의 번거로움을 얼만큼 감당할 것인지 그 선을 정해야 합니다. <디지털 보안을 위한 7가지 원칙>의 <단순할수록 안전하고 쉬워진다>에서 이야기한 것처럼, 이 정도는 단순하고 쉬운 보안 절차라고 감당할 수 있는 수준이 어느 정도인지를 정해야 하는 것입니다.

모든 종류의 정보, 모든 종류의 통신에 동일한 수준의 보안이 필요한 것은 아닙니다. 정부기관을 상대로 디지털 보안 사건 소송을 진행 중인 변호사가 소송 관련 정보를 안전하게 관리하는 경우와, 같은 변호사가 귀여운 고양이 영상을 친구들과 함께 보려고 공유하는 경우는 완전히 다를 수 있습니다.

> 대응해야만 하는 위협에 대응하기 위해 취할 수 있는 선택지를 정리해 봅시다.
> 편의성과 불편함의 경계, 비용의 측면, 기술적 한계 등을 명료하게 나눠봅시다.

현 시점의 '우리 편'과 의논할 사항은?

<디지털 보안을 위한 7가지 원칙>의 <전체 과정에서 가장 취약한 지점을 찾아라>에서 이야기했듯, 대부분의 디지털 보안 대책은 나 한 사람만의 문제가 아닌 경우가 많습니다. 이메일이나 메신저를 통해 정보가 전달된다면, 이미 그 때부터 정보를 전달받은 상대방의 보안 수준은 우리의 보안 수준에 영향을 줍니다. 마찬가지로 상대방의 디지털 보안 대책이 매우 큰 규모의 자원을 사용하여도 나 혹은 우리 조직의 디지털 보안이 취약하면 '우리 편'에게 폐를 끼치게 됩니다.

누구를 얼만큼 믿을지, 왜 믿어야 하는지를 판단하는 것은 중요한

문제입니다. 클라우드 협업 툴이나 생성형 AI 서비스에서 나 혹은 우리 조직의 정보를 유출할 가능성이 있는지, 혹시 대놓고 이용 약관에서 정보를 유출할 수 있다고 하고 있지는 않은지, 혹은 그 말을 얼만큼 믿을 수 있는지 판단해야 합니다.

> 디지털 보안 대책을 함께 고민할 '우리 편'과 무엇을 의논해야 하는지, 그리고 얼만큼 믿을 수 있는지 정리해 봅시다.

디지털 보안 대책을 정기적으로 점검하기

디지털 보안 위협은 디지털 기기의 변화 및 기술 발전에 따라 나날이 달라지기 때문에, 디지털 보안 대책 또한 한 번 마련하고 끝나서는 안 됩니다. 적당한 시간(6개월, 1년 등)을 두고 기존에 수립한 디지털 보안 대책에서 수정, 보완, 혹은 새로 수립해야 하는 지점이 있는지 반드시 확인하세요.

1-1-4. 실전! 디지털 보안 대책 시나리오: 시민단체 상근활동가 'A'의 디지털 보안 대책

'A'는 한 시민단체에서 상근 활동가로 일하고 있는 사회운동가로, 집회와 시위를 직접 기획하고 홍보하며 참여하는 일상을 보냅니다. 상근활동가 'A'는 <디지털 보안 대책 마련하기>의 6가지 질문을 읽으면서, 자신만의 디지털 보안 대책을 마련하기로 하였습니다.

6가지 질문과 함께 보안 대책의 초안 잡기

'A'의 업무 시간 대부분은 컴퓨터와 스마트폰을 이용한 온라인 활동과 집회, 시위 참여로 이뤄집니다. 구글 독스(Google Docs) 및 구글 드라이브(Google Drive)를 사용하여 문서를 만들고,

공유하고, 보관합니다. 카카오톡을 사용하여 시민단체의 동료들과 소통합니다. 홍보 활동을 위해 단체의 인스타그램 등 SNS 계정을 운영합니다. 물론 사적인 개인 SNS 계정도 운영합니다. SNS에는 활동에 관한 내용 뿐만 아니라 사적인 이야기를 올립니다.

'A'는 온라인상의 활동 전반을 보호하기 위한 디지털 보안 대책을 마련할 생각입니다.

'A'의 활동은 정부나 특정 기업과 마찰을 빚곤 합니다. 특히 집회나 시위 계획, 캠페인 계획이 이들에게 전달되지 않았으면 합니다. 또한 'A'는 인터넷 커뮤니티에서 건설적인 토론이 아닌 인신공격성 협박을 받는 경우도 있습니다. 'A'를 위협하는 이들에게서 정보를 지키고 싶습니다.

'A'의 활동과 'A'가 참석하고 기획하는 집회 및 시위는 때때로 불법의 여지가 있습니다. 불법의 여지가 없다 하더라도 정부기관이나 기업에게 빌미를 줄 수 있습니다. 이러한 법적 공방은 그 자체로 A의 생활과 활동에 지장을 줄 것입니다.

'A'가 활동하는 단체는 오로지 시민들의 후원으로만 운영됩니다. 그렇기에 디지털 보안에 추가적인 돈을 투자하는 것은 쉽지 않습니다. 하지만 약간의 불편함을 감수하거나, 기존의 앱과 프로그램을 바꿀 의향은 있습니다.

메신저 바꾸기: 카카오톡 → 텔레그램 → 시그널

'A'는 2014년 카카오톡 압수수색 사건 이후, 메신저 서비스를 제공하는 회사가 정부의 감시에 협조함으로 인해 발생할 수 있는 위험에 대비하고자 텔레그램 메신저를 사용해 왔습니다. 카카오톡과 대비해 상대적으로 한국 정부의 압수수색 등에서 안전할 수 있다는 판단에서입니다.

디지털 보안 대책 수립을 위한 정보 조사에서, ‘A’는 텔레그램에서 ‘비밀채팅’ 을 사용하지 않는 경우 종단간 암호화를 지원하지 않고, 텔레그램 서버에도 메시지가 무기한 저장된다는 점을 알게 되었습니다. 이는 스마트폰을 바꿔도 기존 대화내용을 전부 열람할 수 있는 점에서 편리해 보였지만, ‘A’는 과거의 대화 내용이 대화를 나눈 상대방 외에 텔레그램 서버에도 남아있는 것이 걱정되었습니다.

> 시그널 사용에 추가적인 비용이 필요하지 않고 기능 상 텔레그램과 큰 차이가 없다는 점을 고려하여, 활동과 관련된 소통은 시그널 메신저로 진행하기로 했습니다.

계정 분리와 2단계 인증(2FA) 활성화

‘A’의 활동은 특정 클라우드 회사(구글)에 의존적인 부분이 많았습니다. ‘A’는 하나의 구글 계정으로 다양한 서비스를 사용합니다. 서점, 쇼핑몰, 스트리밍 서비스, SNS 등에 로그인할 때 구글 계정을 사용하여 편리했습니다. 활동에 사용하는 여러 클라우드 협업 툴도 하나의 계정을 사용했습니다.

하지만 이로 인해, ‘A’의 디지털 보안은 구글 계정 하나만 유출되어도 큰 문제가 됨을 확인하였습니다. 특정 클라우드 회사에게 정부가 관계 법령에 따라 ‘A’에 대한 자료를 요구하거나, 해커가 오직 ‘A’의 해당 클라우드 계정만 집요하게 노릴 수도 있습니다.

찬찬히 검토한 결과, ‘A’는 해당 클라우드 회사 자체를 적으로 돌릴 가능성이 낮고, 해당 클라우드 회사 또한 먼저 나서서 ‘A’ 몰래 ‘A’가 주고받은 이메일, 문서 내용 등을 열람할 가능성은 낮다고 판단했습니다. 대신 클라우드 계정 자체의 보안은 높여야 한다는 결론에 이르렀습니다.

> 여러 고민 끝에 'A'는 구글 계정 로그인에 2단계 인증을 설정했습니다. 설령 'A'의 구글 계정 비밀번호를 누군가 알아내도, 2단계 인증에서 막을 수 있게 되었습니다.

> 그리고 'A'는 일상용 계정과 업무용 계정을 분리하기로 하였습니다. 구글 계정을 하나 더 만들고, 업무용 협업툴에는 새로 만든 구글 계정만 사용하기로 하였습니다.

스마트폰 암호화 강화

종단간 암호화 메신저를 이용해도 그 기록이 스마트폰 내에 암호화되지 않은 채 남아있다면, 혹은 스마트폰 화면을 제3자가 볼 수 있다면 문제가 될 수 있음을 알게 되었습니다. 또한 'A'의 스마트폰에서 USIM을 빼내 복제폰을 만들어 'A'에게 오는 연락을 가로챌 수 있다는 것도 알게 되었습니다.

> 이에 'A'는 스마트폰의 USIM에 비밀번호를 설정했습니다. 설령 누군가 'A'의 스마트폰을 몰래 빼내도 USIM 비밀번호 때문에 복제 폰을 만들기 어려워 졌습니다.

> 'A'는 스마트폰 잠금 화면에도 비밀번호를 설정하였습니다. 설령 압수수색을 당하거나 도난을 당해도 'A'가 직접 잠금 화면을 풀지 않는다면 공격자가 함부로 스마트폰 안의 데이터에 쉽게 접근할 수 없게 되었습니다.

비밀번호 관리 도구 도입과 비밀번호 변경

'A'는 비밀번호를 어딘가에 적어두지 말고 머릿속으로 외워야 한다는 조언을 듣고, 자신이 외울 수 있는 비밀번호를 사용해 왔습니다. 하지만 디지털 보안 가이드를 읽으면서, 영어와 숫자로만 구성된

8자리 비밀번호는 보안에 매우 취약함을 알게 되었습니다.

외우기 쉬우면서 길이가 매우 긴 비밀번호를 쓰고 싶었지만,
한국의 웹사이트 중 상당수는 비밀번호의 길이 자체에 제한이
있었습니다. 이에 'A'는 다음과 같은 결정을 내렸습니다.

> 짧은 길이의 비밀번호만 지원하는 경우에 대해, 'A' 대신
> 비밀번호를 외워주는 비밀번호 관리 도구(Password Manager)를
> 사용하기로 했습니다. 'A'는 윈도우와 안드로이드를 사용하므로
> KeePassXC와 KeePassDX를 사용하기로 했습니다.

> 'A'의 비밀번호 관리 도구를 통제하는 마스터 비밀번호는 'A'가 좋아하는
> 노래 가사를 사용하여 50글자 정도로 길게 만들었습니다. 개별 웹사이트에
> 대한 비밀번호는 KeePassXC가 만들어 준 것을 사용하기로 하였습니다.

집회/시위 참석시 생체 인증 비활성화

'A'는 집회 및 시위에 참석할 때 실시간 상황 공유와 SNS 활동을 위해
스마트폰을 들고 다녀야 합니다. 하지만 연행 가능성, 분실 가능성,
압수 가능성 등의 위험에 충분히 대비해야 함을 알게 되었습니다.

> 이에 'A'는 집회 참석 전에 스마트폰의 보안 설정 중, 특히 'A'가 원하지
> 않더라도 보안이 풀릴 수 있는 상황을 항상 점검하기로 하였습니다.
> 평상시 지문 인식을 사용하여 스마트폰을 빠르게 잠금 해제하던
> 'A'는 집회 참석 중에는 이를 비활성화하기로 하였습니다.

사진, SNS에 위치정보 남기지 않기

'A'는 스마트폰으로 사진을 촬영할 때 사진에 위치 정보가 저장되고,

카카오톡 등의 메신저에서 사진을 원본 파일로 공유하면 이러한 위치 정보가 그대로 파일에 남은 채 전달됨을 알게 되었습니다. ‘A’는 ‘A’의 집에서 찍은 사진에 담긴 위치정보로 인해 ‘A’가 원치 않는 개인정보(집의 위치)가 유출될 수 있음을 알게 되었습니다.

> 이에 ‘A’는 위치정보 및 기타 개인정보와 관련된 설정을 모두 공유하지 않기로 하였습니다. 구체적으로 개인적인 사진을 공유하기 전, 메타데이터가 남아있지 않도록 만들고 의도치 않게 실시간 위치를 알리지 않게끔 주의하기로 하였습니다.

링크와 첨부파일은 검증된 경우에만

‘A’는 메신저나 SNS에서 신원이 확실하게 보증되지 않은 이로부터 받는 링크, 첨부파일을 열지 않기로 했습니다.

1-1-5. 실전! 디지털 보안 대책 시나리오: 시민단체 상근활동가 ‘A’의 디지털 보안 대책 2

시간이 흘러 ‘A’는 정기적으로 해 오던 디지털 보안 대책 점검의 시간을 갖게 되었습니다. ‘A’의 상황이 많이 달라졌고, 달라진 상황에 맞추어 ‘A’의 디지털 보안 대책에도 변화가 생겼습니다.

노션 계정을 역할에 맞게 분리

‘A’가 새로 옮겨간 시민단체는 하나의 노션 계정을 여러 활동가가 공유하고 있었습니다. 노션 계정에 단체 내부용 회의록, 단체 외부에 공개할 공지 페이지를 편집할 권한이 모두에게 있었습니다. 이에 ‘A’가 합류하면서, ‘A’는 새로운 시민단체에서의 노션 계정 사용이 잠재적인 위험을 가짐을 느꼈습니다.

> ‘A’와의 논의 끝에, 새로 옮긴 시민단체는 노션 계정을 역할별로 분리하고 각 계정마다 적절한 권한을 부여하게 되었습니다.

시그널 메신저 보안 강화

‘A’는 최근 시그널 메신저를 통해 소통하던 활동가 두 사람의 채팅창에 “OOO 님과의 안전 번호가 변경되었습니다.”라는 메시지가 뜨는 것을 확인했습니다. 한 활동가는 실제로 휴대전화를 바꾼 상황이었고, 다른 활동가는 휴대전화를 분실하면서 새로운 스마트폰에는 시그널 메신저를 아직 설치하지 않은 상황이었습니다.

> ‘A’는 시그널 메신저의 ‘안전 번호 검증’ 기능을 사용하여 두 활동가를 개별적으로 만나 시그널 메신저의 대화 상대가 본인이 맞는지 확인하였고, 앞으로도 확인 작업을 항상 진행하기로 하였습니다.

새로운 휴대전화에 맞는 디지털 보안 도입

‘A’는 기존에 사용하던 휴대전화가 너무 오래되어 새로운 휴대전화를 사용하기로 하였습니다. A는 새로운 휴대전화를 고민하면서 디지털 보안과 관련된 옵션을 검토했습니다.

새로운 아이폰은 집회, 시위 참석 시 유용해 보이는 ‘차단 모드’(Lockdown Mode)를 지원하고, 새로운 삼성 안드로이드 스마트폰은 이와 비슷한 ‘최대 제한 기능’을 지원함을 알게 되었습니다. 차단 모드와 최대 제한 모드는 스미싱 공격 등이 집중될 때 휴대전화 보안 수준을 높이는 데 도움이 된다는 것을 알게 되었습니다.

> ‘A’는 새로운 아이폰에 도입된 ‘차단 모드’(Lockdown Mode)에

대해 충분히 검토하고, 스미싱 공격이 집중되고 있는 시기나 집회 시위 참석 시 차단 모드 사용을 추가하기로 하였습니다.

1-1-6. 실전! 디지털 보안 대책 시나리오: 시민단체 상근활동가 'B'의 선택

'A'는 다른 시민사회단체 상근활동가 'B'를 만나 서로의 디지털 보안 대책을 비교해보는 시간을 갖게 되었습니다. 이 과정에서 'A'와 다른 가치판단을 하는 'B'의 사례들을 살펴보게 되었습니다.

블루투스 및 '내 기기 찾기' 기능에 대한 입장 차이

'B'는 블루투스 기기를 전혀 사용하지 않기 때문에 언제나 블루투스 기능을 비활성화해두고 있습니다. 블루투스 이어폰 등을 사용하는 'A'와 달리, 'B'는 블루투스 기기를 전혀 사용하지 않습니다. 또한 'B'는 빅테크 기업이 '잃어버린 기기 찾기', '내 기기 찾기'등의 명목으로 대중의 위치 정보를 수집하는 것, 심지어 기기의 전원이 꺼져 있더라도 블루투스 신호를 송출시키고 그 기기의 근처를 지나갈 때 이를 다른 기기가 감지하고 수집할 수 있도록 강제하는 기술에 대해 원론적인 문제의식을 갖고 있습니다.

'A'는 기기를 잃어버린 경우 해당 기기를 찾을 수 있거나, 아니면 최소한 원격으로 해당 기기에 저장된 정보를 삭제할 수 있기를 바랍니다. 이런 관점에서 'A'는 빅테크 기업이 이용약관 등에 명시한 내용을 준수한다는 전제 하에, 기기를 잃어버렸을 때 이를 찾아주거나 혹은 원격으로 데이터를 삭제하는 기능을 활성화해두고 있습니다. 반면 'B'는 스마트폰 등 휴대하는 기기에 저장하는 정보를 최소화하고, 기기를 분실하여도 기기를 되찾을 필요성 자체를 최소화하는 삶의 양식을 따르고 있습니다.

블루투스 기기를 사용하는지, 그리고 블루투스 신호에 기반한

위치 정보의 수집에 대해 원론적으로 얼마나 강경한 입장을 취할 지에 대해 'A'와 'B'는 서로 다른 가치판단을 하고 있습니다.

생성형 AI를 비롯한 AI 기술 사용에 대한 입장 차이

'B'는 빅테크 기업이 생성형 AI 등의 학습 및 훈련에 임의로 데이터를 사용할 가능성이 높다고 판단합니다. 설령 그들이 악의를 갖지 않더라도 그들의 실수로 인해 기밀성이 높은 데이터가 유출될 가능성이 조금이라도 있다면 안심할 수 없다고 보고, 생성형 AI를 비롯한 AI 기술을 사용하지 않습니다.

한편 'A'는 생성형 AI 서비스를 제공하는 업체들의 이용약관을 면밀히 살핍니다. 이용약관 자체에 거짓을 명시하지는 않았을 것으로 가정하고, 이용약관에서 밝히는 입장을 신뢰합니다. 빅테크 기업 'C'는 이용약관을 통해, 자사의 생성형 AI 서비스의 학습 및 훈련을 위해 'C'의 서비스를 사용하는 고객들의 데이터를 익명화하여 활용한다고 명시하고 있습니다. A는 빅테크 기업의 익명화 기술의 수준이 높지 않다고 보고, 'C'의 생성형 AI 서비스를 통해 원치 않는 데이터가 유출될 가능성이 있다고 판단합니다. 빅테크 기업 'D'는 이용약관에서 '유료서비스'의 경우 사용자의 데이터를 학습이나 훈련에 사용하지 않는다고 명시합니다. A는 업무생산성 등에 대한 고민 끝에, 필요한 경우 제한적으로 빅테크 기업 'D'의 생성형 AI 유료서비스를 사용하는 것으로 입장을 정리합니다.

'A'는 빅테크 기업들이 이용약관을 어기지 않게 하고, 이용약관 자체에서 드러내고 있는 기술적 한계를 잘 이해하는 데 초점을 두고 있고, 활동가 'B'는 빅테크 기업들에 어떠한 악용의 여지도 주지 않는 데 초점을 두고 있습니다.

클라우드 사용에 대한 입장 차이

'B'는 생성형 AI 이외에도 대부분의 클라우드 협업 도구를 사용하지

않습니다. 디지털 기기를 사용함에 있어 어떠한 정보도 클라우드 업체에 전달되지 않기를 희망합니다. 마이크로소프트의 윈도우나 애플의 맥은 기기를 사용하려면 마이크로소프트나 애플의 클라우드 계정을 기본적으로 만들어야 합니다. 'B'는 이러한 상황에 동의하지 않습니다.

이에 'B'가 사용하는 PC는 리눅스 OS만을 사용하고, 'B'는 마이크로소프트나 애플 아이클라우드 계정 같은 것을 전혀 만들지 않고 있습니다. 또한 안드로이드 스마트폰에도 구글의 플레이 스토어를 사용하지 않습니다. 'B'는 스마트폰에 앱을 설치할 때에도 구글의 플레이 스토어에 의존하지 않고 설치할 수 있기를 원합니다.

> 활동가 'B'는 이런 측면에서 애플의 스마트폰을 사용하지 않고, 좀더 빅테크 기업 등에 의존적이지 않은 방법으로 스마트 기기를 사용할 수 있기를 희망합니다.

보안 메신저에 대한 입장 차이

'B'는 한동안 '종단간 암호화'를 보장하는 파일 공유 메신저로 Keybase 라는 메신저를 사용해 왔습니다. 2020년에 Keybase 가 Zoom에게 인수된 뒤로, 'B'는 더 이상 Keybase를 사용하지 않습니다. 굳이 Keybase를 사용하지 않더라도 Matrix 같은 대안을 찾을 수 있다는 판단에서입니다. 활동가 'B'는 Zoom을 불신하고, 자신이 불신하는 회사가 소유한 Keybase 서비스를 사용하는 것보다는 협업하는 동료들의 IT 전문 지식 수준을 좀더 높여서 동료들이 직접 Matrix 서버를 운영하는 것이 바람직하다고 생각합니다.

> 특정한 회사의 과거 이력에 따른 신뢰, 불신의 이유를 각자 판단하고, 활동가마다 시민마다 판단의 차이가 있음을 이해해야 합니다.

1-2. 디지털 보안 위협 사례와 대책

디지털 보안 대책을 마련하기 위한 평가를 진행하려면 디지털 보안 위협의 실현 가능성을 좀더 잘 알아야 합니다. 한국에서 실제로 빈번하게 일어나는 디지털 보안 위협 사례들과 이에 대한 대책을 마련하는 방법을 알아봅시다.

1-2-1. 시민사회단체 활동가를 노린 스미싱 공격

2024년 9월, 국내 한 정당의 당대표가 텔레그램 스미싱 공격에 의해 계정을 탈취당하는 사건이 발생했습니다.[6] 텔레그램 메신저는 '비밀대화' 기능을 사용하지 않을 경우 모든 대화의 내용이 텔레그램 클라우드에 영원히 저장되기 때문에, 계정 탈취가 일어나면 기존의 대화 내역 등이 모두 공격자에게 노출됩니다. 공격자는 기존 대화 내역을 토대로 탈취한 계정의 신원을 사칭하며 다음 공격대상에 대한 신뢰를 확보하여 추가 피해를 양산할 수 있습니다.

> 텔레그램 메신저를 사용하는 경우, 이러한 공격으로부터 사전에 계정을 보호하기 위해 디지털 보안 가이드 <5-2-4 텔레그램(Telegram) 설정 가이드>를 참고하여 텔레그램을 좀더 안전하게 사용하세요.

텔레그램의 '비밀대화' 기능으로 지켜지지 않는 보안 영역 경계하기

많은 사람들이 텔레그램 메신저를 '보안 메신저'라고 생각합니다. 텔레그램 메신저는 서비스 운영 주체가 한국에 소재하지 않고 있어 서버에 대한 압수수색 영장 집행 등이 어렵다는 점에서 상대적으로 주목받고 있고, 또한 '비밀대화' 기능을 사용할 경우 서버에는 대화 내용

6 https://x.com/Kr_Justice/status/1840719013959344589

본문이 저장되지 않고 오직 메시지를 주고받은 당사자의 스마트폰에만 대화 내용이 저장된다는 점이 주목받고 있습니다. 하지만 이러한 '비밀 대화' 기능을 사용하더라도, 등 뒤에서 어깨 너머로 스마트폰 화면을 지켜보고 있는 제3자로부터 대화 내용의 보안을 지킬 수는 없습니다. 등 뒤에 벽으로 가로막혀 있거나 하지 않다면, 뒤에 있는 사람의 각도에 따라 얼마든지 대화 내용이 유출될 수 있음에 유의해야 합니다.

> 디지털 보안의 본질은 <가장 약한 연결고리>에 있고, 그 가장 약한 연결고리는 물리적인 공간 그 자체에 있을 수 있다는 점을 유의합시다.

1-2-2. 국가기관의 영장 범위 밖 정보수집

2024년 4월, 한 대법원 판결을 통해 대검찰청 D-NET의 운영실태가 또 다시 알려졌습니다.[7] 법원에서 발급한 압수수색 영장에서 제한한 범위를 넘어서는 휴대전화 데이터 전체를 우선 D-NET에 저장하고, 이를 활용할 여지가 있음이 포착된 것입니다. 여러 가지 법적인 이유로 인해 실제로 수사에 활용할 수 없고 오직 원본 기기와의 동일성 및 위조, 변조가 없었음을 보장하기 위해 휴대전화 데이터 전체의 사본을 만들 수 밖에 없다는 정부의 설명이 있지만, 이러한 설명만으로 영장의 범위를 넘어서는 정보 수집을 정당화할 수는 없습니다.

> 휴대전화 데이터가 D-NET 에 저장되더라도 데이터가 유출될 가능성을 최소화하기 위해서는 휴대전화 잠금화면 보안 설정 등을 통해 휴대전화 자체의 데이터 암호화 기능이 작동하고, 저장되어 있는 개별적인 파일 또한 별도의 암호화로 보호되는 상황을 마련해야 합니다. 디지털 보안 가이드 4장을 참고하여 개별 파일, 파일이 저장되는

7 https://www.hani.co.kr/arti/society/society_general/1138282.html#cb

| 볼륨, 기기 차원의 암호화를 상시화할 수 있도록 해 봅시다.

1-2-3. 물리적 보안을 위협하는 디지털 기술 발전

디지털 보안에 대한 최선의 선택으로 디지털 기기를 아예 사용하지 않는 방법을 떠올릴 수 있습니다. 하지만 2024년에 발표된 최신 연구들에서는 열쇠구멍에 열쇠가 들어가는 소리를 AI로 분석하여 복제 열쇠를 만들어내거나, 사람의 말소리가 컵과 같은 식기에 일으키는 진동을 Lidar 센서(자율주행 자동차 등에 많이 사용되는 센서)등을 사용하여 유출해내는 기법 등이 이미 실현되고 있습니다.[8] 이러한 형태의 공격을 모든 공격자가 모든 대상을 향해 언제나 실행할 수 있는 것은 아니지만, 디지털 기술의 발전에 따라 물리적 보안이 충분히 위협에 처할 수 있음을 인지해야 합니다.

| 디지털 보안이 실제 물리세계의 보안과 연결된다는 점을 기억합시다.

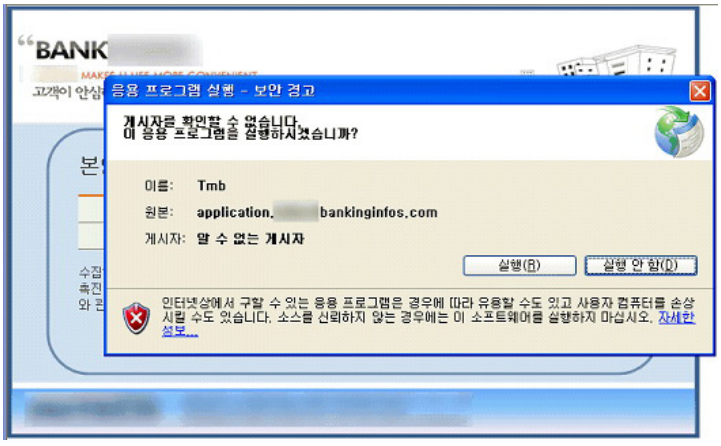
1-2-4. 보안 경고를 무시하고 무지할 것을 강요받아온 한국 인터넷

한국의 인터넷 환경은 Active-X라는 기술을 기반으로 한 특수한 보안 방식을 오랜 시간동안 사용해 왔습니다. Active-X 기술이 폐지된 현재에도 인터넷뱅킹, 관공서 업무 등을 위해서는 대부분의 경우 컴퓨터에 특수한 전용 프로그램을 설치해야만 하는 경우가 많습니다.

문제는 이 과정에서 운영체제(OS) 등의 무수한 보안 경고를 '무시'하라는 방향으로 시민들에게 안내된 경우가 많다는 것입니다. 많은 경우 인터넷뱅킹 등의 사용자 매뉴얼에서는 '보안 경고'가 나타나도 이를

8 https://m.boannews.com/html/detail.html?idx=133004

무시하고 안내하는 경우가 빈번했고, 이로 인해 사용자들이 무시해서는 안 되는 보안 경고와 무시해야 하는 보안 경고를 구분하기 어려운 지경에 이르렀습니다.[9] 예를 들어, 아래와 같은 사진을 살펴보겠습니다.



이 사진의 내용은 컴퓨터의 사용자 스스로가 특정한 프로그램을 실행할지 실행하지 않을지를 판단할 것을 요구하고 있습니다. 상당수 인터넷뱅킹 보안 가이드는 이러한 화면이 나왔을 때 무비판적으로 [실행] 혹은 [허용]을 누를 것을 권고하고 있습니다. 바로 이러한 지점에서 취약점이 등장하고, 사람들의 나쁜 습관이나 버릇을 노린 디지털 보안 공격이 이뤄집니다. 프로그램을 실행할 경우 컴퓨터를 손상시킬 수도 있다, 게시자를 확인할 수 없다, 정말 믿어도 되는지 안 되는지를 사용자가 직접 판단하고 책임져 달라는 내용에 대해, 많은 사용자들이 스스로 이를 판단할 수 있는 능력을 갖추도록 하는 방향이 아닌, 무비판적으로 실행하도록 하는 방향으로의 진행이 이뤄져 온 것입니다.

9 https://it.chosun.com/news/articleView.html?idxno=2014062485029

<아는 만큼 지킬 수 있다>는 원칙을 잊지 말고,
하나씩 하나씩 알아가도록 합시다.

1-3. 보안 도구 선택의 기준

디지털 보안 위협이 갈수록 높아지면서 어떤 도구를 사용해야 디지털 보안 위협에 대처할 수 있는지에 대한 중요성 또한 나날이 높아지고 있습니다. 다양한 도구가 쏟아지고 있기 때문에 어떤 도구를 선택해야 좋을지 고민하게 됩니다. 디지털 보안 그 자체를 위한 도구뿐만 아니라 협업 등 업무에 사용하는 도구를 이하에서는 '보안 도구'라고 부르겠습니다. 어떤 보안 도구를 선택할 지를 고려할 수 있는 몇 가지 기준은 다음과 같습니다.

보안은 '무엇을 고르느냐'의 문제가 아니라 '어떤 과정을 만드느냐'의 문제

<디지털 보안을 위한 7가지 원칙>과 <디지털 보안 대책 마련하기>에서 가장 중요한 것 중 하나는, 디지털 보안은 단순히 어떤 도구(기기, 앱, 서비스 등)를 사용하느냐의 문제가 아니라, 그러한 도구들을 사용하는 과정 전반 그 자체라는 것입니다.

어떤 도구나 소프트웨어도 모든 상황에서 감시로부터 절대적인 보호를 제공하지 못합니다. <전체 과정에서 가장 취약한 지점을 찾아라> 원칙을 다시 떠올려 봅시다. 스마트폰에는 온갖 종류의 디지털 보안 앱을 설치하여도 정작 컴퓨터(PC)에는 비밀번호조차 설정하지 않았다면 어떻게 될까요? 당신의 정보를 탈취하려고 하는 공격자는 스마트폰이 아닌 당신의 컴퓨터를 노릴 것이고, 스마트폰에 설치된 온갖 보안 앱은 컴퓨터를 노리는 디지털 보안 위협에 별 도움이 되지 못합니다. 공격자는 쉬운 길을 두고 어려운 길을 택할 필요가 없기 때문입니다.

<실제로 위협이 일어날 가능성은?>에서 다뤘던 것처럼, 디지털 보안 대책을 마련하는 과정에서 도출된, 실제 대비해야 하는 위협이 무엇이냐에 따라

만들어야 하는 과정은 달라지기 마련입니다. 극단적인 예시를 들어보자면, 만일 법적으로 종단간 암호화(E2EE)가 적용된 통신을 사용하는 것이 금지된 나라의 활동가와 소통해야 하는 상황이라면, 종단간 암호화가 적용된 보안 메신저를 사용하는 것보다는 오히려 사전에 약속된 암호를 사용하는 것이 훨씬 안전합니다. 겉으로 봐서는 암호인지 알 수 없지만 규칙을 아는 사람끼리 규칙에 맞춰 작성하고 해독할 수 있는 암호를, 누구든 도청할 수 있는 문자메시지 등 암호화되지 않은 통신 수단을 사용하여 소통하는 것이 전체 과정을 좀더 안전하게 유지할 수 있는 경우도 있다는 말입니다.

보안 도구의 개방성과 투명성

디지털 보안 전문가들은 개방성과 투명성이 더 안전한 보안으로 이어진다는 강한 믿음을 갖고 있습니다.

<디지털 보안 가이드>에서 권하는 보안 도구들의 특징 중 하나는 오픈 소스(Open-Source), 혹은 자유 소프트웨어(Free Software)라는 것입니다. 이는 소프트웨어의 코드가 공개되어 다른 사람들이 검사, 수정, 공유할 수 있다는 것을 의미합니다. 프로그램의 작동 방식을 투명하게 공개함으로써, 이러한 보안 도구의 개발자들은 다른 사람들로 하여금 보안 결함을 찾아내고 프로그램을 개선할 수 있도록 장려합니다.

주의할 점은 오픈 소스 소프트웨어가 더 나은 보안을 제공할 기회를 제공하지만 이를 반드시 보장하지는 않는다는 점입니다. 소스 코드가 공개되어 있고 대중적이고 유명한 프로젝트라는 것이 반드시 보안 전문가들에 의해 검증이 되었다는 것을 의미하지는 않는다는 점에 유의하세요.

따라서 도구를 고려할 때 소스 코드가 공개되어 있는지,

그리고 독립적인 보안 감사 절차를 통해 어느 정도의 보안성이 검증되었는지를 확인해 보세요. 최소한 소프트웨어나 하드웨어는 다른 전문가들이 검사할 수 있는 작동 방식에 대한 상세한 기술 설명이 제공되는 것을 선택하는 것이 좋습니다.

보안 도구의 장단점에 대한 명확한 공개 여부

어떤 소프트웨어나 하드웨어도 완전히 안전하지는 않습니다. 도구의 개발자, 혹은 도구를 판매하는 업체가 해당 도구의 한계를 얼마나 명확히 공개하는지 판단해보는 것이 좋습니다.

단순히 "군사용" 보안, 혹은 "NSA로부터 안전"(혹은 국가정보원으로부터 안전)하다는 식의 과대 광고는 아무런 의미가 없음에 유의해야 합니다. 이런 식의 표현은 제작자가 자신들의 제품에 대해 지나치게 과신하고 있음, 혹은 보안 취약점을 놓치고 있을 가능성을 드러냅니다.

공격자들은 항상 도구의 보안을 뚫기 위한 새로운 방법을 찾아내기 때문에, 소프트웨어와 하드웨어는 새로 발견된 취약점을 수정하기 위해 항상 업데이트가 필요합니다. 보안 취약점을 개선하기 위한 업데이트가 이뤄지지 않고 방치되면 공격자들이 이를 이용할 것이므로, 보안 업데이트는 지속적으로 이루어져야 한다는 것을 항상 염두에 두어야 합니다. 어떤 보안 취약점이 발견되었고 이를 개선하는 보안 업데이트가 이뤄지고 있음을 투명하게 공개하고 업데이트를 수행하는 도구를 택해야 하는 이유입니다.

보안 도구 개발자의 미래 행동을 예측하는 좋은 방법 중 하나는 그들의 과거 활동입니다. 도구를 소개하는 웹사이트에 올라와 있는 과거의 보안 취약점 목록과 정기적인 업데이트 및 정보, 예를 들어 마지막 소프트웨어 업데이트 이후 얼마가 지났는지에 대한 정보 등이

지표가 됩니다. 지속적으로 업데이트가 끊임없이 이뤄지고 있는지 등이 중요한 정보입니다. 홈페이지, 애플 앱스토어 혹은 구글 플레이스토어 등의 앱 마켓, 오픈소스라면 깃허브(Github) 등의 소프트웨어 코드 저장소, 또는 개발자의 웹사이트에서 업데이트 기록을 확인할 수 있습니다. 업데이트 기록이 존재하고, 또한 구체적으로 어떤 업데이트를 진행했는지에 대한 정보가 제공되고 있는지를 살펴보세요.

보안 도구의 제작자 자신이 보안 위협이 될 가능성 검토

여러분이 만드는 디지털 보안 대책에 활용되는 도구를 만드는 보안 도구 제작자들은 여러분과 마찬가지로 그들 자신을 위한 명확한 디지털 보안 대책을 수립할 것입니다. 많은 경우 우수한 디지털 보안 도구를 만드는 제작자들은 그들이 수립한 디지털 보안 대책의 일부를 투명하게 공개합니다. 이 도구를 사용할 때 어떤 종류의 공격자에게서 어떤 방식의 보호를 제공할 수 있는지를 명시적으로 설명합니다.

하지만 디지털 보안에서는 항상 최악의 경우를 고려해봐야 합니다. 디지털 보안 대책에 활용될 보안 도구의 제작자 자신이 보안 위협이 되는 경우 말입니다. 디지털 보안 도구의 제작자 자신이 위험에 처하거나, 그들이 직접 사용자를 공격하기로 결정하면 어떤 일이 일어날 지 고려해 봐야 합니다. 예를 들어, 법원이나 정부가 보안 도구의 제작자에게 '사용자들의 개인 정보를 제공할 것'을 명령하거나, 혹은 해당 보안 도구의 보안 기능을 우회할 수 있는 뒷문, 즉 '백도어'를 만들 것을 강요할 수 있습니다. 따라서 어떤 도구를 사용할 지 고려할 때, 도구의 제작자가 따라야 하는 법적 관할권이 어떻게 되는지 고려해야 합니다. 예를 들어 당신이 이란 정부로부터 위협을 받고 있다면, 미국 기반의 회사는 이란 법원의 명령을 거부할 수 있을 것입니다. 물론 미국 법원의 명령은 따랴아 하겠지만요.

정부를 비롯한 공권력의 압박만이 문제는 아닙니다. 만일 제작자가 정부의 압박을 견딜 수 있다고 하더라도, 공격자는 유망한 보안 도구 공급 기업의 소비자(즉, 도구 사용자) 전반을 노리고 제작자의 시스템 자체를 공격하려고 시도할 수 있습니다.

이러한 보안 위협에 가장 잘 대처할 수 있는 도구는 이러한 공격을 실제로 일어날 만한 위험으로 간주하고 이에 대한 대책이 수립되어 있는 도구입니다. 예를 들어 메신저를 선택하고자 할 때, 사용자가 나눈 대화를 열람하지 않는다고 주장하는 메신저를 찾기보다는, 이러저러한 이유로 사용자가 나눈 대화를 열람할 방법이 없다고 근거와 함께 설명하는 메신저를 선택하는 것이 좋습니다. 도구의 이용약관이나 개인정보 보호 정책에서 데이터 암호화, 데이터 보존 정책, 제3자에 대한 판매 여부를 어떻게 설명하고 있는지 확인해야 합니다.

보안 도구에 대한 최신 평판 확인

디지털 보안 7가지 원칙의 <오늘 안전했다고 내일도 안전한 것은 아니다> 원칙을 잊지 마세요. 처음에는 안전했던 제품이, 시간이 흐르면서 먼 훗날 심각한 보안 취약점이 있는 것으로 드러날 수도 있습니다. 지금 사용중인 도구들에 대한 최신 정보를 접할 수 있도록 노력하세요. 어떤 종류의 보안 취약점이 밝혀져 이로 인해 어떤 공격이 일어나고 있는지, 그러한 공격에 어떻게 대응해야 하는지에 대한 정보를 쉽게 확보할 수 있는 방법을 마련하세요.

디지털 보안 대책 마련하기의 <현 시점의 '우리 편'과 의논할 사항은?> 질문을 잊지 마세요. 개개인 스스로가 자신이 사용하는 모든 디지털 보안 관련 도구에 대한 최신 소식을 지속적으로 파악하는 것은 많은 노력을 필요로 합니다. 같은 디지털 보안 관련 도구를 사용 중인 '우리

편’과 함께 지속적으로 최신 정보를 공유할 수 있도록 하세요.

어떤 스마트폰, 어떤 컴퓨터를 사야 할지 고민이라면?

디지털 보안에 대한 가장 많은 질문 중 하나가 “안드로이드폰과 아이폰중 어느 쪽이 더 안전한가요?”같은 질문입니다. 혹은 “윈도우가 안전한가요, 아니면 맥이 안전한가요?”같은 질문을 받기도 합니다. 이런 질문에 대한 간단한 답변은 없습니다. 소프트웨어와 기기의 상대적인 안정성은 새로운 보안 취약점이 발견됨에 따라, 발견된 보안 취약점이 해결되고 새로운 보안 기술이 도입됨에 따라 계속 변화합니다. 회사들은 더 나은 보안을 제공하기 위해 서로 경쟁할 수도 있고, 혹은 보안을 약화시키라는 정부의 압력에 놓여있을 수도 있습니다. 따라서 이러한 질문들에 정답은 없습니다.

다만 많은 경우 일반론은 대개 진실에 가깝습니다. 보안 업데이트를 하지 않으면, 모든 디지털 기기는 안전하지 않고, 이 디지털 기기를 안전하게 사용하려면 어떻게 해야 하는지를 고민하는 것이 좀더 낫다는 것입니다. 특히 보안 업데이트가 더 이상 이뤄지지 않는 디지털 기기를 계속 사용하는 상황은 반드시 피해야 합니다. 예를 들어 윈도우를 사용한다면 윈도우 XP, 윈도우 7 등은 더 이상 보안 업데이트가 진행되지 않고, 새롭게 발견되는 보안 취약점이 고쳐지지 않은 채 방치됩니다. 이러한 경우 별도의 보안 도구를 사용하더라도 운영체제 자체의 보안 취약점으로 인해 공격자로부터 안전하지 못할 가능성이 매우 높아진다는 점에 유의해야 합니다.

1-4. 일어날 수 있는 공격의 형태

디지털 보안에서 일어날 수 있는 공격의 형태는 매우 다양하고 방대합니다. 공격 대상이 될 수 있는 것과 간단한 방법으로 공격 대상을 보호할 수 있는 것이 무엇인지에 대해서도 마찬가지입니다. 흔히 일어나는 디지털 보안 공격에 어떤 것이 있는지를 간단히 살펴봅시다.

1-4-1. 인증 수단과 계정 탈취

클라우드 서비스를 비롯한 다양한 인터넷 서비스들은 본인만이 접근할 수 있어야 하는 정보, 예를 들어 이메일 등에 접근하는 과정에서 계정명(아이디)과 비밀번호 등을 사용하여 접근 권한이 있는 사람임을 인증하는 절차를 마련해두고 있습니다. 제2장 <비밀번호와 인증의 실제>에서 비밀번호를 비롯한 여러 가지 인증 수단에 대해 소개합니다.

디지털 보안 위협 중 인증 수단 탈취의 위협은 계정 탈취로 이어지며 상황에 따라 궤멸적인 피해를 일으킬 수 있습니다. 대부분의 디지털 보안의 출발점이 인증으로부터 시작되기 때문입니다. 인증에 사용되는 수단이 탈취당할 경우, 인증 그 자체를 방어 수단으로 사용하는 상황들이 모두 무력화되기 때문에 인증 수단을 보호하는 것은 그만큼 중요한 일입니다.

계정 탈취를 위해 일어나는 공격 중 하나가 스미싱입니다.
해당 (클라우드 등)서비스의 공식 요청을 사칭하여 인증 수단(비밀번호, 2단계 인증 등) 정보를 입력하게 하는 방식이 사용됩니다. 특히 SNS, 메신저, 암호화폐 지갑 등 인증 수단이 탈취될 때 사생활이나 정보유출, 자산유출 피해가 심각하게 일어나는 곳을 대상으로 한 스미싱 피해가

매년 급증하고 있습니다. 2024년에도 점점 더 커져가는 피해에 따라 한국인터넷진흥원 등의 국내 관계기관에서도 계정 탈취를 경계하라고 안내하고 있습니다.[10] 앞서 <시민사회단체 활동가를 노린 스미싱 공격>에서 살펴본 바와 같이, 메신저 등을 노린 공격이 특히 가속화되고 있습니다.

때로는 비밀번호가 암호화되어 저장되어 있는 서버의 데이터가 유출되기도 합니다. 흔히 '고객정보 유출사고'라고 불리는 보안 침해사고가 일어나는 경우가 여기에 속합니다. 비밀번호가 암호화되는 방식에 따라 비밀번호 원문이 복원될 수도 있습니다. 여러 웹사이트에 동일한 비밀번호를 사용하고 있다면, 동일한 비밀번호를 사용하는 웹사이트 중 가장 보안이 취약한 웹사이트에서 비밀번호가 유출되는 사고가 일어나는 순간 해당 비밀번호를 동일하게 사용하는 웹사이트, 혹은 클라우드 서비스의 계정 정보 또한 그대로 탈취될 위험에 처하게 됩니다.

인증 수단으로 보호되고 있는 곳이 단체나 조직의 웹사이트라면, 계정을 탈취한 사람이 웹사이트의 내용을 변조하는 상황이 발생할 수도 있습니다. 우리 단체의 웹사이트에 방문하는 모든 사람들의 컴퓨터에 악성 코드를 설치하도록 하는 일이 일어난다면 큰일입니다. 우리 단체의 웹사이트에 우리 단체의 명의로 우리 단체의 입장과는 정반대되는 입장문이 게시되거나 하여도 혼란을 초래할 수 있습니다.

1-4-2. 자료, 정보, 데이터 유출 및 변조 공격

메신저를 통해 주고받은 메시지나 이메일을 통해 주고받은 이메일, 첨부파일, 인증을 거쳐야만 접근할 수 있는 웹 사이트 내부에 게시된

10 https://www.boho.or.kr/kr/bbs/view.do?searchCnd=&bbsId=B0000133&searchWrd=&menuNo=205020&pageIndex=1&categoryCode=&nttId=71555

정보, 혹은 스마트폰이나 컴퓨터에 저장되어 있는 파일의 내용 자체를 알아내기 위한 공격은 가장 떠올리기 쉽고 가장 빈번하게 일어나는 디지털 보안 공격입니다. 특히 2024년처럼 클라우드 기반 협업 툴, 혹은 클라우드 기반 서비스에 대한 의존성이 커져가는 시대에는 이러한 클라우드 서비스에 저장된 정보를 유출하기 위한 공격 시도가 더더욱 커지고 있습니다. 단순히 정보를 외부로 유출하는 것 뿐만 아니라 파일 내용 일부를 조작하거나 파일을 손상시키는 변조 등의 공격도 횡행합니다.

파일의 내용을 유출하려는 공격으로부터 데이터를 보호하기 위한 수단이 몇 가지 있습니다. 하나는 파일을 암호화하여 저장하는 것입니다. 복호화 수단이 없는 사람에게는 설령 파일이 유출되더라도 파일의 내용까지 즉시 유출되는 상황을 막을 수 있습니다.
파일을 첨부할 때 파일을 그대로 첨부하지 말고, 7-Zip 등의 압축 프로그램을 사용하여 특정한 비밀번호를 알고 있는 사람만 압축을 해제할 수 있도록 암호화하는 것이 한 가지 방법입니다.

| <4-1 파일과 저장기기>를 참고하여 파일을 적절히 암호화하세요.

파일을 하나씩 개별적으로 암호화하는 방법은 주로 파일 한두 개를 일회성으로 전송하는 경우에는 충분히 사용할 만하지만, 단체나 조직 내에서 기밀로 관리되어야 하는 많은 파일들이 있을 때 일괄적으로 적용하기 어렵습니다. 제4장 <파일과 저장기기>에서 소개하는 볼륨 암호화 방식 등을 참고하여, 볼륨 단위에서 암호화된 채로 저장되게 하는 것이 한 가지 방법입니다.

데이터가 변조되거나 삭제되지 않도록 보호하려면 백업, 즉 별도의 저장장치에 사본을 마련해 두는 것이 한 가지 방법입니다. 이런 경우 마련해

둔 사본 자체가 유출되거나 도둑맞지 않도록 신경써야 합니다. 또한 데이터의 백업 과정에서 악성 코드가 함께 백업되거나 하지 않도록 주의가 필요합니다.

1-4-3. 통신 내용의 도·감청 및 통신 기록의 감시

인터넷을 통해 전송되는 정보는 암호화되지 않을 경우 정보의 전송 경로에 있는 그 누구든지 정보의 내용을 열람할 수 있는 구조를 갖고 있습니다. 이를 노리고 공공장소 등에 정보 수집을 목적으로 하는 와이파이 장비를 설치해 두고, 이 와이파이 장비를 거쳐가는 모든 암호화되지 않은 데이터 전송을 도청하는 공격이 이뤄집니다. 굳이 와이파이 장비를 별도로 설치하지 않더라도 회사 네트워크 설비 차원, 혹은 국가에 따라서는 통신사 등 인터넷 회선 공급자 차원에서의 전방위적인 도청이 기술적으로 가능한 상황이 마련되기도 합니다.

이러한 도청 등으로부터 통신 내용을 보호하기 위해서는 다양한 준비가 필요합니다. 통신 당사자 간에 상호 인증을 하는 것이 그 시작입니다. 통신을 시작하기 전에 통신의 양 주체가 서로를 올바른 통신 대상인지 확인하고 서로만이 정보를 주고받을 수 있는 형태로 암호화를 하여 정보를 주고받는 것이 출발점입니다. 이러한 통신이 이뤄지기 위해서는 통신의 각 주체가 스스로를 인증할 수 있는 수단과 방법이 마련되어야 하며, 웹 사이트의 경우 TLS 인증서라는 것을 통해 현재 방문중인 사이트가 해당 사이트가 맞다는 것을 인증하는 과정 등이 수반됩니다.

물론, 이러한 암호화 과정을 거치더라도 통신사 차원에서는 여전히 특정 기기가 어느 시각에 어떤 기기와 소통을 했는지에 대한 정보를 추적할 방법이 있고, 때로는 이러한 정보 자체가 통신 기록의 감시 대상이 되곤 합니다. 이러한 감시로부터 안전한 통신을 할 방법이 마련되어야 합니다.

VPN 사용, 혹은 Tor 네트워크 사용 등이 대책이 될 수 있습니다.

1-4-4. 키로거(KeyLogger) 등의 악성 코드와 클립보드 모니터링

아이디와 비밀번호를 이용한 인증 방식은 기본적으로 아이디와 비밀번호가 제3자에게 유출되지 않는다는 가정을 전제로 한 인증 방식입니다. 만일 사용자가 키보드의 어떤 키를 언제 어느 시점에 어떻게 눌렀는지를 모니터링할 수 있다면, 이 모니터링을 하는 주체에게 아이디도 비밀번호도 유출되지 않을 방법이 마땅치 않게 됩니다. 물리적인 키보드에 어느 키가 눌렸는지, 혹은 스마트폰 화면에 키보드가 표시될 경우 화면의 어느 영역을 몇 시에 터치했는지에 대한 정보에 접근할 수 있다면 비밀번호가 유출되는 것은 시간 문제로 전락해 버립니다.

공공장소의 컴퓨터 등 나 자신이 디지털 보안 수단을 충분히 통제할 수 있는 상황에 놓여있지 않은 환경에서는 비밀번호 등을 이용한 로그인 시도 자체가 해당 컴퓨터에 설치된 악성 코드, 혹은 여러 가지 변수에 의해 심각한 보안 취약점으로 작용할 수 있습니다.

편의성을 위해 사용자가 (클립보드에) '복사'한 내용을 모니터링하고 있는 앱들이 있습니다. 사용자가 '복사'하는 내용이 보안에 큰 위험이 되지 않는 정보라면 문제될 일이 없겠지만, 보안에 중요한 대화 내용을 다른 사람에게 전하기 위해 잠깐 '복사'한 내용이 다른 앱에게 전달된다면 큰 문제가 됩니다. <완벽한 보안은 없고, 언제나 타협점이 있음을 명심하라>는 보안 원칙에서 이야기했듯, 편의성 증진을 위한 몇 가지 기능들은 오히려 보안 취약점이 될 수 있음을 알아야 합니다.

1-4-5. 물리적 보안, 인적 보안

디지털 보안과 물리적 보안, 인적 보안은 떼려야 뗄 수 없는 관계입니다. 디지털 기기에 저장된 정보를 열람하고 통제하는 것이 결국은 사람이고, 사람이 디지털 기기에 저장된 정보를 보는 과정에서 물리적인 실체를 거치기 때문입니다. 디지털 정보가 저장되어 있는 기기 자체의 보안, 정보가 오고가는 경로 즉 인터넷 연결을 이뤄주는 장비 자체의 보안, 디지털 기기와 사람 사이의 물리적 공간 자체의 보안, 정보에 대한 접근 권한이 있는 사람 자체의 보안 등이 유기적으로 맞물려 돌아갑니다.

아무리 우수한 보안 메신저를 사용하여 음성 통화를 진행한다고 하더라도, 다른 사람이 들어서는 안 되는 민감한 내용을 공공장소에서 이야기하고 있다면, 내 바로 가까이에서 내 목소리를 들을 수 있는 제3의 인물에게 대화 내용이 유출되는 것을 피할 수 없습니다. 또한 이러한 상황을 모두 막을 수 있는 방식을 찾아 정보 소통을 하더라도, 정작 나 자신이 혹은 대화의 상대방이 정보를 유출하는 상황 혹은 그에 준하는 상황이 온다면 이 또한 디지털 보안의 취약한 지점으로 남게 됩니다.

단체의 구성원 간에 비밀번호를 공유하고 있다면, 단체의 구성원에 변동이 생길 때 해당 비밀번호를 유지하는 것이 바람직한지가 문제가 됩니다. 또한 단체의 구성원이 되기 위해 오랜 시간을 들여 신뢰를 쌓아올리는 유형의 공격자에게 취약한 상황을 초래할 수도 있습니다.

스마트폰의 잠금을 지문 인증만으로 해제할 수 있게 하면 자고 있는 동안 누군가가 내 지문을 사용하여 스마트폰의 잠금을 해제하는 것을 막을 수 없습니다. 스마트폰의 잠금을 패턴으로 해제한다면 스마트폰의 화면에 남아있는 터치 흔적을 토대로 패턴을 추리하는

방식의 공격을 막을 수 없습니다. 비밀번호를 나의 신원정보와 밀접하게 관련이 있게 설정한다면 나의 신원정보에 접근할 수 있는 다른 사람이 나의 비밀번호를 추리해내는 것을 막을 수 없습니다. 여전히 많은 사람들이 자신의 비밀번호와 자신의 신원정보, 즉 자신의 생년월일이나 연인의 생년월일, 혹은 가족의 전화번호 등을 연관지어 두기 때문에, 이러한 지점을 노리는 디지털 보안 공격은 여전히 유용합니다.

마지막으로, 화면 캡쳐나 녹음이 불가능하다고 안내하는 여러 가지 보안 도구들은 스마트폰의 화면 자체를 제3의 카메라로 촬영하는 방식, 혹은 스피커폰 등을 사용하여 소리가 외부로 나가도록 하고 그 소리를 별도의 마이크 장비를 사용하여 녹음하는 방식으로부터 방어해줄 수 없습니다.

1-5. 디지털 보안, 예방과 대응

제1장에서는 디지털 보안에 대한 여러 원칙들과 기초 지식들을 살펴봤습니다. 디지털 보안 대책 수립에 있어 예방도 중요하고, 대응도 중요합니다. 충분히 존재할 수 있지만 과소평가되는 위험 중 하나가 '실수'에 의한 보안 위협입니다. 각종 절차를 마련하여 실수가 이뤄지지 않도록 실수를 예방하는 예방일변도의 대책이 언제나 좋은 결과물을 가져오지는 못할 수도 있다는 것입니다.

예를 들어, 미국 산림청에서는 산불이 전혀 일어나지 않도록 아주 조그마한 불씨도 무조건 다 없애는 식으로 산림 관리를 하다 보니 오히려 숲이 전반적으로 엄청나게 건조해져서 산불이 한번 터졌다 하면 엄청나게 큰 산불이 나는 상황이 관찰된 바 있습니다. 이에 따라 산림청의 정책 방향은 모든 종류의 산불을 막는 것을 벗어나 감당할 수 있는 규모의 산불이 나는 걸 허용을 하는 방향으로 바뀌고 있습니다. 감당할 수 없는 커다란 사고가 일어나는 일을 막으려면, 모든 사고를 막기보다 오히려 사고가 일어났음을 기민하게 알아차리고 빠르게 대응하는 게 낫다는 관점으로의 패러다임 전환이 이뤄지고 있는 것입니다.

비밀번호 보안의 경우에도 마찬가지입니다. 비밀번호를 무조건 주기적으로 바꾸는 것이 맞을까요? 아니면 내 비밀번호가 노출되었다는 것을 알게 되면 그 시점에 바꾸는 것이 맞을까요? 중요한 것은 디지털 보안 침해 사고가 일어나지 않도록 예방하는 것뿐만 아니라, 사고가 일어난 시점에 대응할 방법이 있어야 하고 또한 사고가 일어났음을 알 수 있어야 한다는 것입니다.

이러한 관점들을 염두에 두고, 여러분의 디지털 보안을 강화해 나가시기를 바랍니다.

2. 비밀번호와 인증의 실제

디지털 보안으로 지켜야 하는 대상에 접근할 수 있는 자격이 있음을 증명하게 하는 것이 디지털 보안의 시작입니다. 이러한 증명(인증)에서 가장 많이 사용되는 방법은 계정의 ID와 비밀번호를 확인하는 것입니다.

2024년에는 비밀번호가 아닌 다른 인증방식도 광범위하게 사용되고 있습니다. 지문이나 얼굴 등 생체 정보를 이용하기도 하고, 특정한 디지털 기기를 갖고 있는지를 확인하기도 합니다. 각각의 인증 방식이 어떤 면에서 안전하고 어떤 면에서 위험한지 살펴봅시다.

2-1. 비밀번호

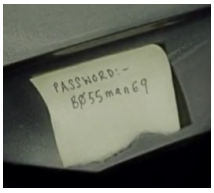
비밀번호는 '지식 기반 인증'(Something You Know)입니다. 디지털 환경에서 어떤 사람이 "내가 아니면 모를 비밀번호를 내가 알고 있다. 그러니 내가 (이메일이나 메신저 혹은 자신의 기기에) 로그인하게 해 달라"는 용도로 활용됩니다. 숫자, 문자, 혹은 특수기호로 구성합니다. 일반적으로 '문자의 나열'(문자열)의 형태가 됩니다. 당연히 다른 사람이 쉽게 짐작할 수 있는 문자열은 비밀번호로 가치가 없습니다. 비밀번호는 그 자체가 '비밀'이어야 합니다. 한국어로는 숫자 4자리 등의 형태가 은행 계좌, 신용카드 등에 사용되면서 '비밀번호'라는 표현이 정착되었는데, 영어로는 부호(번호)의 나열이라는 뜻에서 Passcode, 번호 외에 문자를 포함하게 되면서 Password, 단어 한두 개 수준의 길이가 아닌 형태가 가능해지면서 Passphrase 등 표현의 변천사가 있어왔습니다.

안전하지 않은 비밀번호와 안전한 비밀번호에 대해 구체적으로 살펴봅시다.

2-1-1. 비밀번호가 안전하지 않은 이유

비밀번호 '인증' 과정에 대한 이해

스티븐 스필버그의 SF 영화 '레디 플레이어 원'에 등장하는 사람들은 하루의 대부분을 메타버스(Metaverse) 가상현실 세계인 '오아시스(OASIS)'에서 보냅니다. 오아시스에 접속할 땐 접속하려는 계정의 비밀번호를 알아야 하고, 비밀번호만 알면 인증(Authentication) 절차는 끝납니다. 영화 속 악당은 비밀번호를 항상 기억할 수 있는 특별한 비법을 갖고 있는데요, 바로 사무실의 단말기 안쪽에 포스트잇을



붙여두고 거기에 비밀번호를 적어 두는 것입니다.
다시 강조하지만, 비밀번호는 그 자체가 '비밀'이고, 다른 사람이 쉽게 짐작할 수 없어야 합니다. 포스트잇만 볼 수 있으면 누구든 바로 알 수 있는 비밀번호는 비밀번호로 쓰일 자격이 없습니다.
여기서 '비밀번호'를 다른 사람이 짐작할 수 없어야 한다는 것에는 비밀번호가 맞는지 틀렸는지를 검증하는 주체 또한 그 비밀번호를 짐작할 수 없어야 한다는 것을 뜻합니다. 즉, 비밀번호는 나 자신이 잊어버린다면 그 누구도 알아낼 수 없어야 하고, 비밀번호가 맞는지 틀렸는지를 검증하는 주체조차 오직 지금 입력한 비밀번호가 해당 사용자의 비밀번호가 '맞는지', '틀렸는지'만 알 수 있어야 합니다.

현대적인 비밀번호 기반 인증 방식에서는 대체로 이러한 원칙이 지켜질 수 있도록, 비밀번호를 '단방향 암호화'라는 방식을 사용하여 저장해 둡니다. 그리고 누군가 비밀번호를 입력하면, 방금 입력된 비밀번호를 '단방향 암호화'해 보고, 그 결과물이 과거의 단방향 암호화로 저장된 것과 일치하는지를 검증합니다. 만일 일치한다면 인증을 통과한 것으로 하고, 일치하지 않는다면 인증을 통과하지 못한 것으로 합니다.

안전하지 않은 비밀번호 1: 개인정보와 일치하는 비밀번호

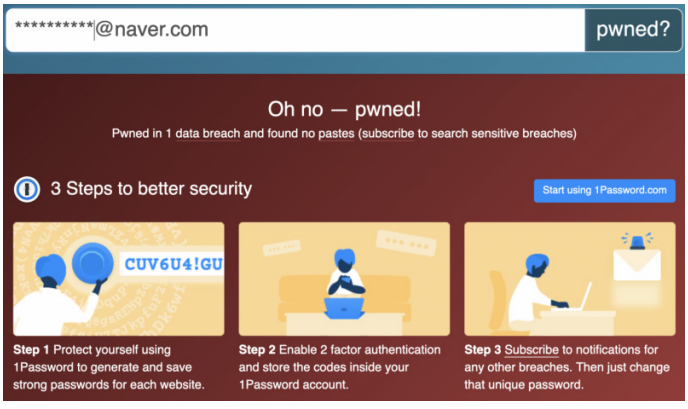
지난 2009년, 경찰은 전국교직원노동조합 및 전국공무원노동조합 조합원들의 민주노동당 가입 여부를 수사하는 과정에서, PC방에서 89개의 주민등록번호를 이용하여 민주노동당 사이트에 접속하는 방식으로 압수수색 영장을 집행한 바 있습니다.[11] 민주노동당에서 일괄적으로 당원들의 접속 계정을 설정하면서 초기 비밀번호를 주민등록번호로 설정하였기 때문에 이러한 작업이 가능했습니다. 수사 기관이 압수수색

11 http://www.newscham.net/news/view.php?board=news&nid=55705

영장 집행을 당사자의 입회 하에 하지 않은 것 자체도 큰 문제이지만, 이처럼 주민등록번호 등을 비밀번호로 사용할 경우 정부기관이나 해커에 의한 공격에 쉽게 노출될 수 있습니다. 따라서 어떠한 경우에도 개인정보와 일치하는 비밀번호를 설정하는 것은 피해야 합니다. 개인정보에 대해 접근이 가능하기만 하면 비밀번호를 알아낼 수 있다는 뜻이 되기 때문입니다.

안전하지 않은 비밀번호 2: 다른 곳에서 유출된 비밀번호

비밀번호 유출 사고는 해가 갈수록 심해지고 있습니다. 개인정보 유출 여부 모니터링 웹사이트 '해브아이빈폰드'(HIBP, ';--have i been pwned?)[12]에는 2022년 4월 20일 기준 117억 건이 넘는 개인정보 유출 사례가 등록되어 있습니다.[13]



서로 다른 비밀번호를 수백 가지 만들고 이를 모조리 기억하는 것은 힘들기 때문에, 디지털 보안 위험에 노출되는 많은 사람들은 서로 다른 계정이나 사이트에서 동일한 비밀번호를 공유하는 경우가 많습니다.

12 https://haveibeenpwned.com/
13 https://www.bloter.net/news/articleView.html?idxno=43865
https://www.bloter.net/news/articleView.html?idxno=44018

당연히 공격자들은 이러한 정보를 공격에 활용합니다. 공격자는 가장 보안이 취약한 계정을 노려 비밀번호를 탈취하고, 만일 피해자가 같은 비밀번호를 다른 곳에 사용하고 있다면 그 계정도 연달아 탈취할 수 있게 됩니다. 즉, 이 비밀번호는 그 비밀번호가 사용된 서비스 중 가장 안전하지 않은 서비스의 보안 수준만큼 위험한 비밀번호가 됩니다.

안전하지 않은 비밀번호 3: 짧고 짐작하기 쉬운 비밀번호

같은 비밀번호를 여러 계정에 걸쳐 동일하게 사용하지 않는 것은 중요한 보안 요구 사항이지만, 인간의 인지 능력의 한계 때문에 서로 다른 비밀번호를 동시에 외우는 것은 불가능에 가깝습니다. 그렇기에 많은 사람들은 짧고, 간단한 비밀번호를 사용하는데, 공격자들은 이를 쉽게 추측할 수 있습니다. 예를 들어 'password1', '12345', 'qwe123'(QWERTY 자판 왼쪽 상단의 키), 생일, 사람 이름 등은 쉽게 추측됩니다.

안전하지 않은 비밀번호 4: 무차별 대입 공격이 진행되고 있는 비밀번호

소설이나 만화 같은 데 주로 나오는 클리셰 중 비밀번호와 관련된 것이 몇 가지 있습니다. 비밀번호가 숫자 4자리라는 사실을 알고 있는 등장인물이 비밀번호를 맞추기 위해 0000, 0001, 0002, 이런 식으로 모든 가능한 경우의 수를 전부 입력해보는 장면입니다. 여행용 캐리어의 3자리 비밀번호를 잊어버리는 일이 잦은 사람들도 자주 하게 되는 행동입니다. 이런 공격방식을 무차별 대입 공격(Brute Force Attack)이라고 합니다.

현대적인 디지털 보안 원칙에서는 바로 이런 무차별 대입 공격으로부터 비밀번호를 안전하게 지키기 위해, 누군가가 비밀번호 입력을 반복적으로 시도하고 반복적으로 실패할 경우 비밀번호 입력 시도를 지속하지 못하고 일정 시간 동안 기다려야만 하도록 하는 절차를 마련할 것을 원칙으로 하고 있습니다. 마치 ATM기 등에서 카드 비밀번호를 여러 번 틀리면

카드를 ATM기가 회수해버리는 것처럼, 무차별 대입 공격을 막기 위한 최소한의 안전장치를 마련할 것을 의무화해두고 있는 것입니다.

하지만 이미 무차별 대입 공격이 진행될 수 있는 상황은 얼마든지 마련될 수 있습니다. 가령 단방향 암호화된 비밀번호와 비밀번호 검증 방법이 들어있는 서버가 해킹된 경우, 공격자는 이렇게 해킹한 '단방향 암호화된 비밀번호'를 '비밀번호 검증 방법'에 따라 검증하기 위해 수십만, 수백만 대의 좀비 PC를 만들어 무차별 대입 공격을 시험해 볼 수 있습니다. 혹은 서버 관리자가 무차별 대입 공격에 대한 방어 장치를 마련해 두지 않은 상황도 상정할 수 있습니다. 어느 쪽이든 비밀번호의 길이가 충분히 길지 않다면, 무차별 대입 공격에 필요한 만큼의 시간이 흐르면 비밀번호를 맞출 수밖에 없습니다.

한국의 비밀번호: 최대 길이 제한

무차별 대입 공격에 필요한 시간을 가능한 한 길게 하려면 비밀번호의 길이는 정말 길어야 하고, 숫자 이외의 다른 글자도 다양하게 사용할 수 있어야 합니다. 컴퓨터의 성능이 좋아지면서 무차별 대입 공격이 가능한 비밀번호의 유형도 과거와 크게 달라졌습니다. 적당한 길이(12글자 이내)이면서 알파벳 대문자, 소문자가 섞여있고 특수문자와 숫자가 반드시 공존해야 한다, 라는 규칙을 따르는 비밀번호의 경우 사람이 외우기는 어려우면서도 무차별 대입 공격에는 취약한 경우가 점점 늘어나게 되었습니다. 사람이 외우기 편하면서도 쉽게 추측할 수 없는 비밀번호는 길이가 길면 길수록 안전해집니다. 하지만 한국의 경우 많은 서비스들이 비밀번호를 최대 16자 정도로만 설정할 수 있도록, 최대 길이를 매우 짧게 제한하고 있습니다.[14]

14 https://help.naver.com/service/5640/contents/1036?lang=ko

입력하다 틀리면 안 되는 비밀번호

비밀번호를 무작정 길고 어렵게 만들면 생기는 문제 중 하나가, 바로 비밀번호를 잘못 입력하는 것입니다. 비밀번호를 여러 번 틀리면 계정이 잠기도록 설정되어 있는 환경에서 20글자 이상의 비밀번호를 입력하다가 중간에 어디서 잘못 입력하였는지를 알 수 없게 된다면 비밀번호를 틀리는 일이 빈번하게 발생해 새로운 보안 문제가 발생하게 됩니다. 비밀번호를 여러 번 틀려서 계정이 잠기고, 잠긴 계정을 풀기 위해 다른 수단을 사용하는 일이 일상화되면 공격자의 공격으로 인해 비밀번호가 틀리는 상황과 나 자신 혹은 나와 계정을 공유하는 누군가가 비밀번호를 틀린 상황을 구분할 수 없게 됩니다.

2-1-2. 비밀번호 관리 도구 사용하기

비밀번호는 근본적으로 결함 투성이인 인증 방식이라고 볼 수 있습니다. 그럼에도 불구하고 비밀번호를 사용해야만 한다면, 몇 가지 선택지가 있습니다. 하나는 상대적으로 안전한 비밀번호를 만들 자신만의 방법을 마련하는 것이고, 또 다른 하나는 <비밀번호 관리 도구>를 사용하는 것입니다. 물론 두 가지는 동시에 적용할 수 있습니다.

비밀번호 관리 도구: 비밀번호들을 안전하게 관리해주는 도구들

비밀번호 관리 도구(Password Manager), 혹은 비밀번호 금고의 목적은 외우기 힘들지만 추측하기 힘든 강력한 비밀번호를 모든 계정마다 다르게 관리하는 데 있습니다. 비밀번호 관리 도구에 저장된 비밀번호를 확인하기 위한 비밀번호를 '마스터 비밀번호'(Master Password)라고 합니다. 마스터 비밀번호만 잘 기억하면, 각각의 비밀번호는 비밀번호 관리 도구가 대신 기억해 주는 방식입니다. 비밀번호 관리 도구 내부의 비밀번호 데이터베이스에 실제로 사용할 비밀번호가 저장됩니다. 예를

들어 'vAeJZ!Q3p$Kdkz/CRHzj0v7'처럼 길면서 사람이 도무지 외울 수 없는 비밀번호도 비밀번호 관리 도구가 대신 기억해 줄 수 있습니다.

비밀번호 관리 도구 사용 여부의 판단

비밀번호 관리 도구의 마스터 비밀번호와 비밀번호 관리 도구의 비밀번호 DB가 유출되면, 비밀번호 관리 도구 속에 넣어둔 비밀번호가 몽땅 유출되는 결과를 가져옵니다. 따라서 비밀번호 관리 도구를 사용할 때에는, 특히 비밀번호 관리 도구 자체의 비밀번호가 유출됨으로 인해 더 큰 피해가 일어날 수 있음을 염두에 두고 판단해야 합니다.

여러 대의 컴퓨터를 사용하거나, 혹은 스마트폰과 컴퓨터를 사용하는 등, 여러 개의 기기에서 동일한 비밀번호 DB를 사용해야 하는 경우가 있습니다. 많은 비밀번호 관리 도구들은 비밀번호 파일을 여러 기기에서 공유할 수 있도록 하는 기능, 즉 '동기화'기능을 제공합니다. 혹은 비밀번호 DB를 클라우드 등의 원격 서버에 저장해 두고, 노트북이든 스마트폰이든 필요할 때 원격 서버에서 비밀번호 DB를 가져오도록 하는 기능을 제공하기도 합니다.

이러한 기능, 즉 클라우드 서버 기반의 비밀번호 동기화 기능을 사용할지의 여부는 결국 각자 수립한 <디지털 보안 대책>에 따라 달라지게 됩니다. 비밀번호 관리 도구 서비스 제공 업체에게 정보 제공을 명령할 권한이 있는 공격자(정부 등)가 운영하는 서버의 경우, 혹은 업체의 클라우드 서버가 해킹당하는 경우 등이 얼마나 발생함직한지를 고려해야 합니다. 최악의 경우 비밀번호 관리 도구 서비스를 제공하는 업체에서는 비밀번호 관리 도구를 당신이 언제, 어디서, 어떤 웹사이트에 대해 사용했는지를 모니터링할 수 있는 가능성 또한 발생할 수 있는데, 이러한 각각의 가능성에 대해서 자신의 디지털 보안 대책이 얼마나 심도

있게 위험으로 고려하는 지에 따라 판단은 달라질 수밖에 없습니다.

많이 쓰이는 비밀번호 관리 도구

비밀번호 관리 도구로 이 가이드에서 소개하는 도구는 윈도우, 리눅스, 맥 등 PC 환경을 위한 KeePassXC, 안드로이드 스마트폰을 위한 KeePassDX, 아이폰을 위한 Strongbox가 있습니다. 이 세 가지 도구는 각 비밀번호 관리 도구에서 사용하는 비밀번호 데이터베이스를 서로 공유할 수 있습니다.

이외에도 구글, 애플, 마이크로소프트 등이 각자 비밀번호 관리 도구를 제공하고 있고, 삼성 등 스마트폰 제조업체에서도 비밀번호 관리 도구 서비스를 운영하고 있습니다. 1password, LastPass 처럼 비밀번호 관리 도구만 전문적으로 운영하는 서비스도 있습니다. 일부 서비스는 유료이고, 클라우드를 이용하여 여러 기기에서 편리하게 비밀번호 데이터베이스를 동기화해주는 경우도 있습니다. 각각의 도구에 대해 얼만큼 신뢰할 수 있는지의 여부는 시점에 따라, 그리고 개개인의 판단에 따라 다릅니다.

2-1-3. 강력한 비밀번호의 요건

처음부터 끝까지 틀리지 않고 기억할 필요가 있고, 특히 강력해야 할 몇 개의 비밀번호가 있습니다. 디지털 보안 가이드를 읽고 수립한 보안 대책에서, 당신의 데이터를 암호화하여 완전히 잠그는 역할을 수행하는 비밀번호들이 여기에 속합니다. 최소한 당신 기기의 비밀번호, 전체 디스크 암호화와 같은 암호화 비밀번호, 그리고 비밀번호 관리자의 '마스터 비밀번호'가 여기에 속합니다. 이러한 성격의 비밀번호들은 다음과 같은 요건을 만족해야 합니다.

길어야 한다

강력한 비밀번호는 길어야 합니다. 외울 수 있는 한 가능한 한 긴

비밀번호일수록 좋습니다. 비밀번호라는 말의 어감은 숫자 4자리 혹은 숫자 6자리 정도로 짧아야 할 것만 같은 인상을 줍니다. 패스워드(낱말) 혹은 패스프레이즈(문장)라는 영어 표현이 뜻하는 것처럼, 길어야 합니다.

복잡해야 한다

강력한 비밀번호는 숫자로만 구성되거나, 혹은 단순한 영어 단어로만 구성되거나 해서는 곤란합니다. 무차별 대입 공격이 일어나도 어느 정도 시간을 버틸 수 있을 정도로는 복잡한 것이 좋습니다.

외울 수 있고 암호화되지 않은 채로는 기록이 남지 않아야 한다

비밀번호는 어딘가에 기록되어 남는 순간 그 기록을 열람할 수 있는 사람 모두에게 노출되기 때문에, 가급적 외울 수 있는 것이어야 합니다. 카카오톡 채팅창 같은 곳이나 이메일 같은 곳에 비밀번호를 적어두면 절대로 안 됩니다.

나의 개인정보와 관련되지 않아야 한다

이름, 주민등록번호, 전화번호, 가족이나 친구의 이름, 생년월일 등 나와 관계된 단어를 사용하지 않아야 합니다.

다른 사람과 공유하지 않아야 한다

나 자신 이외의 다른 사람과 비밀번호를 공유하는 일은 없어야 합니다. 공유하는 순간부터 이미 '비밀번호'가 아니게 됩니다. 단체의 기기의 비밀번호 등 특수한 목적으로 단체 내에서 공유되어야 하는 비밀번호라면, 더 이상 해당 비밀번호를 공유해서는 안 되는 사람이 발생한 경우(단체 구성원의 변동 등) 비밀번호를 바꿀 수 있어야 합니다. 또한 비밀번호를 공유해야만 하는 순간에 제3의 인물이 어깨

너머로 비밀번호를 쳐다보거나 엿듣는 상황이 발생해도 곤란합니다.

다른 계정에서 쓰지 않아야 한다

하나의 계정의 비밀번호가 유출되면 다른 계정의 정보가 위험해지기 때문에, 서로 다른 계정에서 똑같은 비밀번호를 사용하고 있어서는 안 됩니다.

유출되지 않아야 한다

악성 코드 등이 설치되어서 컴퓨터나 스마트기기에 입력하는 비밀번호, 혹은 비밀번호 관리 도구에 설정한 마스터 비밀번호가 유출되는 순간, 비밀번호는 더 이상 비밀번호로 기능할 수 없습니다.

직접 입력하는 경우, 오타 없이 입력할 수 있어야 한다

비밀번호 관리 도구의 마스터 비밀번호처럼 직접 입력해야 하는 비밀번호의 경우, 비밀번호 입력 시 실수나 오타 없이 입력할 수 있어야 합니다. 자신이 사용하는 디지털 기기들에서, 예를 들어 PC의 키보드와 스마트폰의 키보드 양쪽 모두에서 실수 없이 오타 없이 입력할 수 있는 비밀번호를 선택하세요.

2-1-4. KeePassXC 사용법

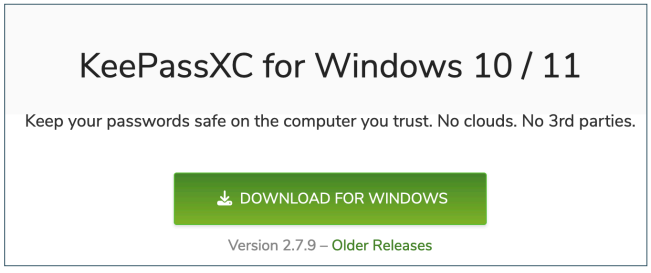
KeePassXC는 비밀번호 관리 도구입니다. 다양한 웹사이트와 서비스에서 쓰이는 당신의 모든 비밀번호를 암호화하여 저장하는데 이용하는 프로그램입니다. 이 훌륭한 도구를 통해 당신은 서비스마다 각각 다르고 추측하기 힘들며 길고 강력한 비밀번호를 사용할 수 있습니다. 당신은 오로지 비밀번호 데이터베이스의 암호를 풀 수 있는 '마스터 비밀번호'만을 기억하면 됩니다.

물론 비밀번호 금고를 사용하는 경우, 공격자는 당신의 비밀번호

금고를 '단일 공격 지점'으로 삼고 어떻게든 비밀번호 금고의 비밀번호 데이터베이스와 '마스터 비밀번호'를 알아내려고 공격을 집중할 수도 있습니다. 완벽한 보안은 없고, 언제나 타협점이 존재한다는 것을 염두에 두고 KeePassXC 사용법을 익혀 봅시다.

KeePassXC 설치하기

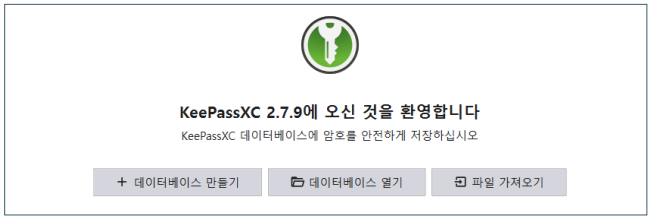
KeePassXC 다운로드 페이지에서 자신의 운영체제에 맞는 파일을 다운받으세요. 윈도우의 경우 별도로 설치하지 않고 바로 실행할 수 있는 포터블 버전도 있습니다.



이 가이드에서는 '설치'를 완료했다고 가정합니다.

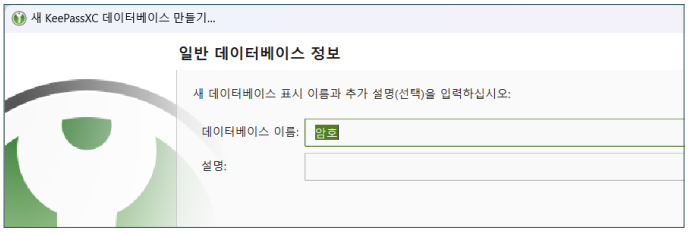
KeePassXC 처음 시작하기

설치한 KeePassXC를 실행합니다. 첫 화면에서 새 데이터베이스를 만들 수도 있고 기존에 사용하던 데이터베이스나 파일을 가져올 수도 있습니다.

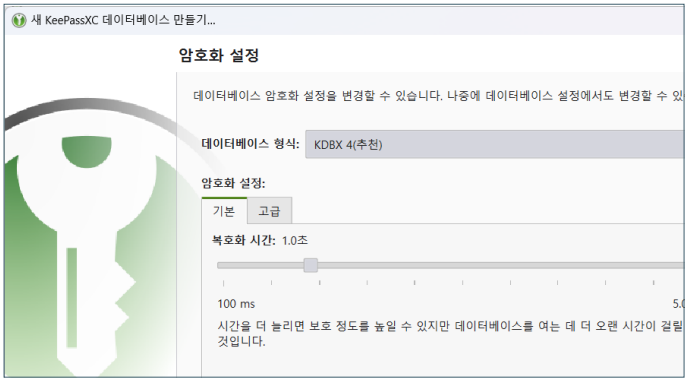


[데이터베이스 만들기]를 선택합니다. 잘 알아볼 수 있도록 새

데이터베이스의 이름을 입력합니다. [설명]은 굳이 적지 않아도 됩니다.



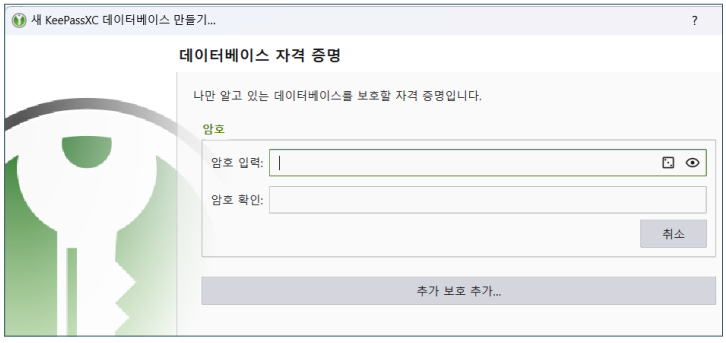
암호화 설정을 통해 복호화에 걸리는 시간과 데이터베이스 파일의 형식을 지정하고 [계속]을 선택합니다. 마스터 비밀번호를 입력한 뒤에 개별 비밀번호를 확보할 수 있게 되기까지 걸리는 시간을 말합니다. 특별히 고민하지 말고 [계속]을 눌러도 됩니다.



이제 마스터 비밀번호를 입력합니다. [암호 입력]과 [암호 확인]에 같은 비밀번호를 입력하면 됩니다. 비밀번호를 입력하는 과정에서 마스터 비밀번호가 얼마나 안전한지 혹은 취약한지를 볼 수 있습니다.

[추가 보호 추가]를 선택하여, 마스터 비밀번호 외에도 특정한 파일을 키 파일로 지정할 수 있습니다. 예를 들어 [키 파일]을

특정한 USB 메모리에만 저장하고, KeePassXC를 쓸 때만 그 USB 메모리를 컴퓨터에 연결한다면 KeePassXC에 저장된 비밀번호를 더 안전하게 관리할 수 있습니다. [키 파일]의 이름이나 위치는 바뀌어도 괜찮지만, [키 파일]의 내용이 절대 바뀌지 않게 주의해야 합니다. [키 파일]의 내용을 사용하여 비밀번호 데이터베이스에 대한 추가 암호화가 진행되기 때문에, [키 파일]의 내용이 조금이라도 변경되면 비밀번호 데이터베이스를 복원할 수 없게 되기 때문입니다.

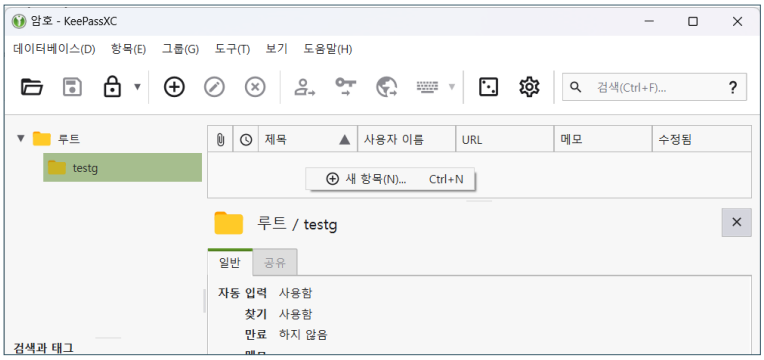


비밀번호 그룹 만들기

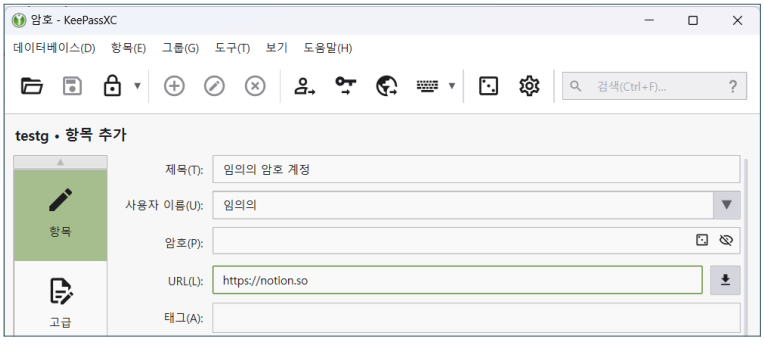
KeePassXC는 기본적으로 여러 개의 비밀번호를 편리하게 관리할 수 있도록 폴더 형식의 '그룹'을 나누어 줍니다. 이를테면 하나의 컴퓨터로 개인적인 일과 업무를 모두 처리한다면, '개인용' 그룹과 '업무용' 그룹 2개를 만들어 둘 수 있습니다. 메뉴바의 [그룹] 버튼을 선택하거나 왼쪽 창에서 마우스 우클릭으로 그룹과 그 하위 그룹을 생성, 삭제, 편집할 수 있습니다.

비밀번호의 저장, 생성, 편집

새로운 비밀번호를 생성하거나, 이미 사용중인 비밀번호를 저장하기 위해서는 원하는 그룹에서 마우스 우클릭을 통해 [새 항목]을 선택합니다. 또는 메뉴바에서 [항목] → [새 항목] 을 선택해도 됩니다.

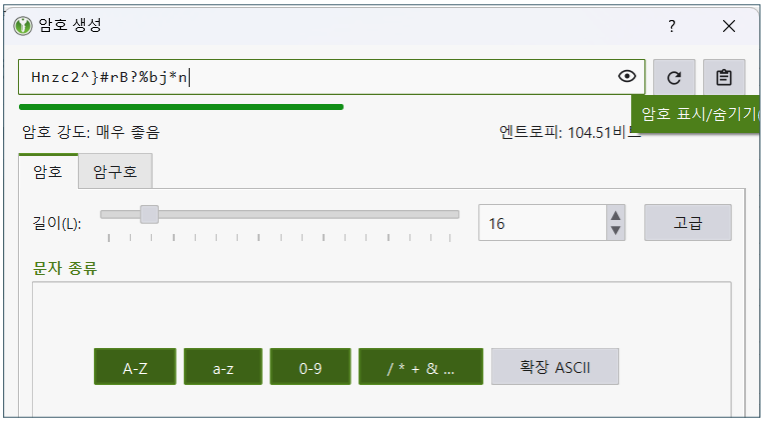


새로운 비밀번호 항목이 무엇에 대한 비밀번호인지 알아볼 수 있도록 [제목]을 적습니다. 예를 들어 단체의 노션(Notion) 계정에 대한 항목이라면 제목은 간단하게 '단체 노션'이라고 적어도 되겠습니다. [사용자 이름]은 해당 비밀번호에 대응되는 계정, 즉 이메일 주소나 ID를 말합니다. KeePassXC가 직접 ID와 비밀번호를 입력하도록 하려면 [사용자 이름]은 정확하게 입력해야 합니다. URL 칸에는 이 비밀번호를 사용하는 서비스의 웹 주소를 입력합니다. 노션이라면 https://notion.so 처럼 하면 됩니다.



[암호]칸의 오른쪽에 있는 주사위 버튼을 클릭하면 KeePassXC가 직접 비밀번호를 만들어 줍니다. 주의할 점은 한국의 경우 비밀번호의 최대

길이를 제한하는 경우가 많다는 점입니다. 예를 들어 2024년 기준으로 네이버의 비밀번호 길이는 16글자로 제한됩니다.[15] 비밀번호의 최대 길이를 제한하고 있는 사이트가 많으므로 이 점에 유의하여 생성시키고, [암호 적용]을 누르면 생성된 비밀번호가 앞 화면의 [암호]칸에 입력됩니다.



지정이 완료되었으면 [확인] 을 선택하여 비밀번호를 데이터베이스에 저장합니다. 변경 사항을 저장하기 위해 메뉴바에서 [데이터베이스 저장]을 선택하여 마무리합니다. 만일 비밀번호를 생성했다면 생성한 비밀번호를 실제로 해당 서비스에서 사용하도록 비밀번호 변경을 해 주세요.

통상적인 이용

비밀번호 데이터베이스의 어떤 항목을 이용하려면 해당 항목을 우클릭하여 [사용자 이름 복사]나 [암호 복사]를 선택 후 아이디와 비밀번호 입력을 원하는 서비스에 가서 '붙여넣기'를 하면 됩니다.

고급 이용

15 https://help.naver.com/service/5640/contents/1036?lang=ko

KeePassXC가 직접 웹 브라우저에 비밀번호를 입력하도록 할 수 있습니다. 모질라 파이어폭스, 토르 브라우저, 구글 크롬, 마이크로소프트 엣지, 비발디, 브레이브 브라우저 등을 사용하는 경우에 가능합니다. 자세한 사항은 KeePassXC 웹 브라우저 통합 플러그인 매뉴얼[16]을 참고하세요.

다른 기능들

메뉴바의 [도구] → [데이터베이스 잠금]을 선택하여 KeePassXC를 잠글 수 있습니다. 이렇게 하면, KeePassXC를 실행된 상태로 놔두더라도 비밀번호 데이터베이스에 다시 접근할 때에 마스터 비밀번호를 입력해야 합니다. 혹은 특정한 시간 동안 이용하지 않으면 KeePassXC가 자동적으로 잠기도록 할 수도 있습니다. 이렇게 하면 잠깐 자리를 비운 사이 누군가가 비밀번호에 접근하는 것을 막을 수 있습니다. 이 기능을 사용하려면, [도구] → [설정]을 선택하여 [보안 항목]을 선택합니다. 그리고 [다음 시간 동안 활동이 없을 때 데이터베이스 잠금] 박스를 체크하고 적당한 시간을 설정합니다.

KeePassXC는 아이디와 비밀번호 외에 다른 것도 저장할 수 있습니다. 예를 들어, 계정 번호, 제품 키, 일련 번호, 혹은 다른 중요한 것들을 저장하기 위해 이용할 수도 있습니다. [암호] 칸에 들어가는 것이 실제 비밀번호일 필요는 없으며, KeePassXC가 대신 외우고 있길 바라는 무엇이든 상관없습니다.

KeePassXC는 2단계 인증 기법 중 TOTP를 지원하므로, <2-2-1 2단계 인증이란?>에서 소개하는 TOTP 2단계 인증을 위한 도구로 활용할 수 있습니다. 다만 KeePassXC를 TOTP 2단계 인증 도구로 사용하고자 할 경우, TOTP를 저장하기 위한 비밀번호

16 https://keepassxc.org/docs/KeePassXC_GettingStarted#_setup_browser_integration

데이터베이스를 별도로 만드는 것을 권장합니다. 그렇지 않으면 하나의 비밀번호 데이터베이스와 이에 대한 마스터 비밀번호가 유출되는 것만으로도 2단계 인증을 위한 TOTP까지 유출될 수 있기 때문입니다.

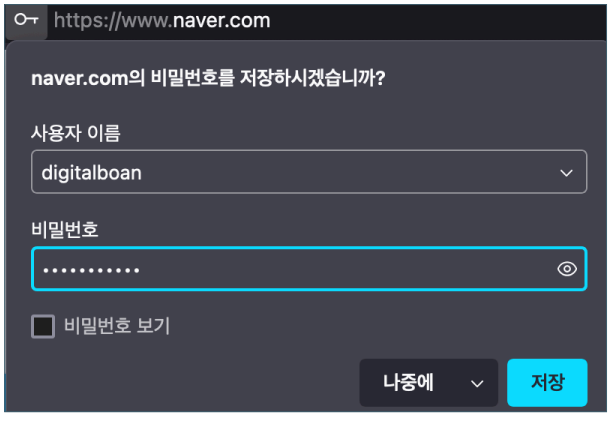
스마트폰 등에서 사용하기

KeePassXC와 호환되는 스마트폰 비밀번호 관리 도구를 사용할 수 있습니다. 안드로이드폰의 경우 KeePassDX[17] 등의 앱을 사용할 수 있으며, 아이폰의 경우 StrongBox[18] 등의 앱을 사용할 수 있습니다.

2-1-6. 비밀번호에 대한 FAQ

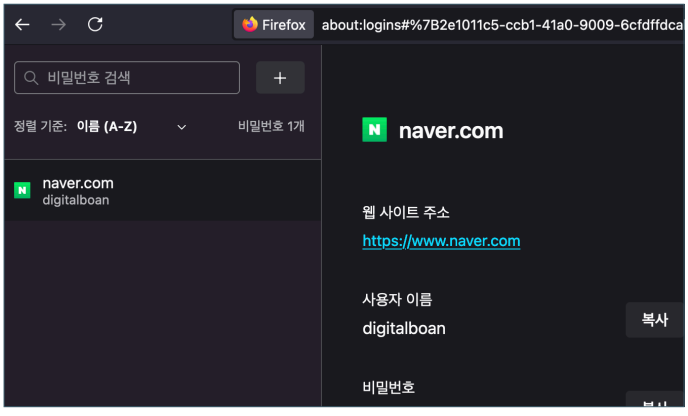
웹 브라우저에 내장된 비밀번호 관리 도구는 쓰면 안 되나요?

많은 웹 브라우저는 사용자가 웹 사이트에 아이디와 비밀번호를 이용하여 로그인하는 상황을 감지하면, 웹 브라우저에 비밀번호를 저장할지의 여부를 물어봅니다. 아래의 사진은 맥에서 실행중인 파이어폭스가 네이버 비밀번호를 웹 브라우저에 저장할지를 물어보는 화면입니다.

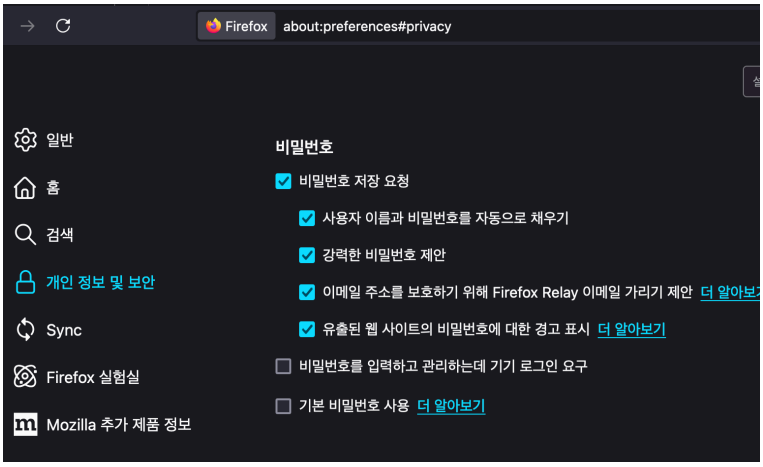


17 https://www.keepassdx.com/
18 https://strongboxsafe.com/

웹 브라우저에 내장된 비밀번호 관리 도구의 안전성은 웹 브라우저마다 큰 차이가 있습니다. 과거 한국에서 주로 사용된 인터넷 익스플로러 등의 웹 브라우저는 사용자가 입력한 비밀번호를 나중에 대신 입력해주는 [자동 완성] 기능을 제공했는데, 컴퓨터를 사용하는 사람이 누구인지 확인하지 않기 때문에 다른 사람에게 잠깐 컴퓨터를 빌려줘도 그 사람이 나쁜 마음을 먹고 [자동 완성] 기능을 사용하여 나의 동의 없이 나의 이메일 등을 확인하는 상황을 막을 수 없었습니다. 통상적인 비밀번호 관리 도구라면 내가 잠시 자리를 비울 때 마스터 패스워드를 입력하도록 요구하도록 설정해서 이런 상황을 막을 수 있었겠지만요. 예를 들어, 아래 사진은 파이어폭스 웹 브라우저에 내장된 비밀번호 관리 도구에서 저장되어 있는 비밀번호를 열람하고 있는 장면을 보여줍니다.



만일 파이어폭스 웹 브라우저에 내장된 비밀번호 관리 도구를 안전하게 사용하고 싶다면, 다른 비밀번호 관리 도구와 마찬가지로 마스터 비밀번호를 설정해야 합니다. 파이어폭스 웹 브라우저에서는 [기본 비밀번호]라고 부릅니다. 기본적으로는 파이어폭스 설정의 개인정보 보안 설정 화면은 아래와 같이 [기본 비밀번호]에 체크가 해제되어 있습니다.



여기서 [기본 비밀번호 사용]을 체크하고 [기본 비밀번호], 즉 마스터 비밀번호를 설정하면 다른 비밀번호 관리 도구를 사용할 때와 비슷하게, 마스터 비밀번호를 알고 있는 경우에만 비밀번호 관리 도구를 사용할 수 있게 됩니다.

인터넷 익스플로러의 사례나 파이어폭스의 사례를 통해 살펴보면, 웹 브라우저에 내장된 비밀번호 관리 도구는 별도의 추가 설정 없이 사용할 경우 웹 브라우저 자체가 나의 비밀번호를 유출할 수 있는 주된 경로로 악용될 여지가 있습니다. 따라서 KeePassXC 등의 별도의 비밀번호 관리 도구를 사용하는 것 대비 어떤 장점, 단점이 있는지 명확히 파악하고 충분히 검토해보세요. 이를테면 오직 나 자신만 사용하는 것이 보장되는 PC에서 업무용 계정과 개인용 계정을 모두 사용하는 경우, 업무용 계정들에서 사용되는 비밀번호는 크로미움 브라우저와 KeePassXC를 사용하고, 개인적인 용무는 파이어폭스 웹 브라우저와 파이어폭스에 내장된 비밀번호 관리 도구를 사용하되 [기본 비밀번호]를 설정해두는 방식도 고려해볼 수 있습니다.

인터넷 익스플로러의 경우 [자동 완성] 기능의 보안이 매우 취약한 것으로 알려져 있습니다. 인터넷 익스플로러의 [자동 완성] 기능에 저장된 암호를 손쉽게 추출하는 악성코드도 있습니다. 물론 마이크로소프트가 인터넷 익스플로러에 대한 기술지원을 완전히 중단하였기 때문에, 2024년의 한국에서 더 이상 인터넷 익스플로러를 사용하는 경우를 찾아보기는 어렵겠습니다. 이처럼 안전하지 않다는 사실이 정평이 나 있는 웹 브라우저에 비밀번호를 저장하는 것은 당연히 위험한 선택입니다.

비밀번호에 한글을 쓸 수 있나요?

한국의 시중 은행 통장이나 신용카드의 비밀번호에는 오직 4자리 혹은 6자리의 숫자만 입력할 수 있지만, 네이버 등의 포털 사이트의 비밀번호에는 숫자 이외에도 영어 알파벳, 특수문자 등을 입력할 수 있습니다. 이처럼 비밀번호에 어떤 문자를 쓸 수 있는지의 여부는 사용중인 웹사이트, 서비스마다 다릅니다.

대개 한국에서는 영어 알파벳을 입력할 때 QWERTY 자판을 많이 사용하고 한글을 입력할 때 두벌식 자판을 많이 사용하기 때문에, 두벌식 자판 기준으로 한글을 입력할 때 대응되는 QWERTY 자판의 영어 알파벳을 입력하게 되는 경우가 많습니다. 이를테면 비밀번호를 '내 비밀번호는 정말 강력해'라고 적고 싶다면 'so qlalfqjsghsms wjdakf rkdfurgo'를 사용하는 식입니다.

이런 특성 때문에 한국에서 사용되는 많은 스마트폰 키보드에서도 비밀번호를 입력하는 화면에서 한글 자판을 입력하면 두벌식 자판, QWERTY 자판 기준으로 대응되는 영어 알파벳을 대신 입력하는 모습을 볼 수 있습니다. 따라서, 현 시점에는 비밀번호에 한글을

직접 쓸 수는 없고 대신 한글 자판에 대응되는 영어 알파벳을 쓰는 경우가 대부분이라고 이해하면 되겠습니다.

비밀번호를 잊어버린 경우, 비밀번호를 알려주지 않는 이유는 무엇인가요?

과거 한국에서는 사용자의 비밀번호를 데이터베이스에 복원 가능한 형태로 저장해 두는 웹 서비스가 상당수 있었습니다. 이러한 서비스들은 '비밀번호 찾기'등의 메뉴를 제공하였고, 사용자가 자신의 신원을 적당한 방법으로 인증하면 '비밀번호'를 이메일로 보내주곤 하였습니다. 하지만 2024년 현재는 이렇게 자신의 '비밀번호'를 알려주는 서비스는 대부분 사라졌습니다.

사용자가 인증을 위해 비밀번호를 입력하면, 많은 경우 비밀번호는 '일방향 해시'같은 특수한 기법을 사용하여 전송됩니다. 데이터베이스에는 이렇게 '일방향 해시'처리된 비밀번호가 저장됩니다. 이후 사용자가 인증을 위해 비밀번호를 입력하면 그 비밀번호를 그대로 사용하지 않고 '일방향 해시'처리된 정보를 이용하여 데이터베이스에 저장된 내용과의 동일성을 검증합니다. 데이터베이스에 저장된 내용만 갖고는 원래의 비밀번호가 무엇이었는지 알아내는 것이 수학적으로 어렵다는 게 보장되는 형태로 저장하기 때문에, 사용자가 비밀번호를 잊어버리면 데이터베이스가 있더라도 그 비밀번호가 무엇이었는지 알아낼 수 없게 되는 것입니다.

비밀번호를 복원 가능한 형태로 데이터베이스에 저장해둔다면 그 데이터베이스가 유출될 때 치명적인 보안 사고가 발생하게 됩니다. 따라서 현재는 '비밀번호 찾기'라는 이름의 기능은 많은 경우 '비밀번호 재설정' 기능으로 대체되어 있습니다. '비밀번호 재설정'은 비밀번호를 분실했지만 자격이 있는 사람임을 다른 방식으로 '인증'한 사람에게 새롭게 비밀번호를 설정할 수 있도록 하는 기능입니다.

정리하면, 비밀번호를 잊어버린 사람에게 비밀번호를 알려줄 수 없는 이유는 현대적인 비밀번호 관리 체계에서는 실제로 서비스 운영 주체가 사용자의 비밀번호를 알아낼 방법이 없기 때문이고, 없어야 하기 때문입니다.

만일 <4-1 파일과 저장기기> 등에서 다루는 파일 등의 '암호화'에 비밀번호를 사용하는 경우라면, 파일의 암호화에 사용된 비밀번호를 분실하면 그 파일의 내용은 영원히 복원할 수 없습니다.

2-2. 2단계 인증과 패스키

2-2-1. 2단계 인증이란?

계정명과 비밀번호만으로 로그인할 수 있게 하는 방식과 달리, 2단계 인증(2-Factor Authentication, 2FA) 방식은 로그인을 하기 위해 비밀번호 이외의 다른 수단, 이를테면 어떤 물리적인 장치를 보유하고 있을 것을 강제하는 방식을 말합니다. 스마트폰 등 항상 지니고 있는 기기를 사용하도록 하는 경우가 많고, 별도의 하드웨어 장비인 '보안 토큰'이라고 부르는 특별한 기기가 사용되기도 합니다.

2단계 인증을 사용하면 설령 비밀번호가 유출되는 일이 발생하더라도, 공격자가 2단계 인증에 필요한 물리적인 장치를 확보하지 못한다면 인증을 통과하지 못하게 됩니다. 즉, 공격자가 당신의 계정에 접근하기 위해서는 당신의 비밀번호는 물론 휴대전화까지 손에 넣어야 하므로 계정 탈취 등의 공격으로부터 좀더 안전해질 수 있습니다.

물론 2단계 인증을 사용하기 위해서는, 인증 대상이 되는 서비스가 2단계 인증 방식을 지원해야 합니다. 2024년 기준 구글, 노션 등 국내에서 활발히 사용되고 있는 클라우드 협업 도구들이 2단계 인증 기능을 지원하고 있습니다.

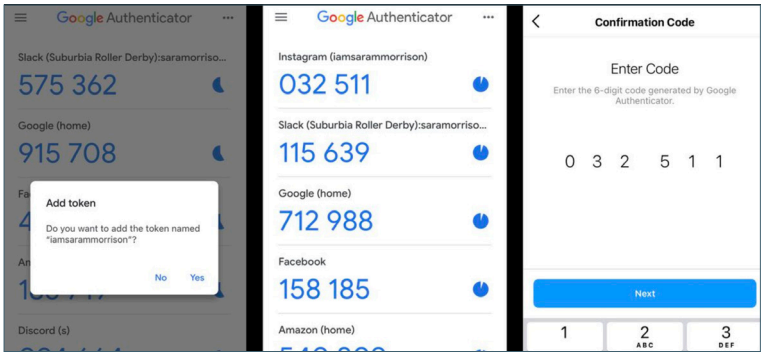
휴대전화를 이용한 '2단계 인증'은 크게 두 가지 방법이 사용되곤 합니다. 당신이 로그인할 때마다 당신의 휴대전화로 SMS 메시지를 보내거나, 휴대전화 자체에서 보안 코드를 생성하는 인증 프로그램을 사용하는 방법이 활용됩니다. 이러한 방법들은 공격자가 당신의 비밀번호는

가지고 있지만, 휴대전화에 물리적으로 접근할 수 없을 때 당신의 계정을 보호하는 데 도움이 됩니다.

전자(SMS 메시지를 보내는 방식)의 휴대전화를 이용한 2단계 인증은 당신의 휴대전화 번호를 서비스 업체에 제공해야 하는데, 이는 개인의 신원을 의도하지 않게 드러낼 수도 있습니다. 특히, 한국과 같이 휴대전화 서비스 이용을 위해 신원 확인을 해야만 하는 경우 이는 민감한 문제일 수 있습니다.

한편 구글이나 노션 등은 시간 기반 일회용 비밀번호(Time-based One-Time Passwords, TOTP) 방식의 2단계 인증을 지원합니다. TOTP를 지원하는 앱을 스마트폰에 설치하고, 이 앱에 제공할 TOTP 정보를 생성해 즉시 TOTP 앱에 등록하면, TOTP 앱은 일정 시간마다 1회용 비밀번호를 만들고, 해당 1회용 비밀번호가 일치할 때에만 2단계 인증이 통과하도록 하는 방식입니다.

KeePassXC, KeePassDX, StrongBox 등의 비밀번호 관리 도구는 TOTP 기능을 지원하며, TOTP 기능만을 수행하는 별도의 앱(Aegis Authenticator, Bitwarden Authenticator, Google Authenticator, Microsoft Authenticator 등)을 사용하여 관리할 수도 있습니다.



여러 사람이 하나의 계정을 공유하는 경우, 2단계 인증을 사용하기 위해서는 2단계 인증의 수단 또한 공유할 수 있어야만 합니다. SMS 메시지를 보내는 방식의 2단계 인증을 사용하려면 누군가 한 사람의 휴대전화번호로 문자메시지를 수신하고, 이를 다른 사람에게 전달해야 하는데 이 과정에서 필연적으로 보안 취약점이 발생할 수 있습니다. TOTP를 사용하고자 한다면 2단계 인증을 위해 TOTP 앱에 QR Code 등을 등록하기 위해, 2단계 인증 수단을 공유해야 하는 기기를 가진 사람들이 한 자리에 모여 TOTP 앱에 정보를 저장해야 합니다. 또한 구성원의 교체 등으로 인해 2단계 인증을 새로 설정해야 할 때 다시 모여야 한다는 점에 유의하여야 합니다.

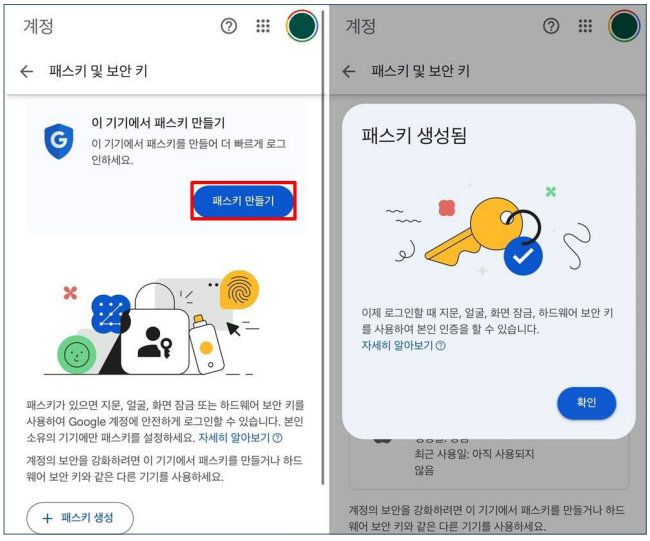
2-2-2. 패스키(PassKey) 등의 새로운 인증 방식에 대한 이해

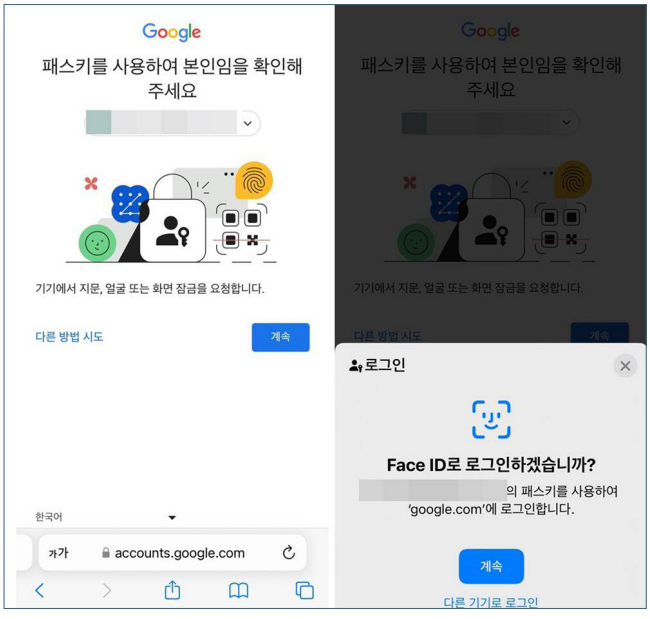
패스키(PassKey)는 비밀번호를 사용하지 않으면서도 안전한 인증방식을 제공하기 위해 도입된 새로운 인증방식입니다.[19]
로그인을 위해서 계정의 비밀번호 대신 항상 당신이 갖고 다니는 스마트폰 등의 기기와 해당 기기를 인증하는 데 쓰일 수 있는 생체정보 혹은 그 기기 자체에 설정한 비밀번호를 사용하도록 합니다.[20] 아래 사진과 같은 과정을 거쳐 구글 계정에 패스키를 설정할 수 있습니다.

패스키는 항상 내 곁에 특정한 기기가 있고, 또한 그 기기에는 오직 나 자신만 풀 수 있는 인증방식이 마련되어 있다는 두 가지 전제를 하고 있습니다. 따라서 패스키가 적용된 기기를 분실하였을 경우, 기존처럼 비밀번호를 이용하거나 혹은 패스키가 적용되어 있는 제3의 기기를 사용하거나 하는 등의 방법으로 계정에

19 https://it.donga.com/104990/
20 https://www.eff.org/deeplinks/2023/10/what-passkey

로그인할 방법이 있다는 전제 하에, 해당 기기에 연결된 패스키를 계정에서 제거하는 식으로 보안 상황을 유지할 수 있습니다.





비밀번호가 전송되는 횟수 혹은 전송되기 위해 입력되는 횟수가 늘어날수록 비밀번호가 유출될 수 있는 가능성은 증가할 수밖에 없습니다.
패스키를 활용하는 방식에 대해 좀더 자세히 알아보려면, 패스키에 대해 소개하는 애플,[21] 구글[22] 등 여러 서비스의 소개문을 살펴보세요.

21 https://support.apple.com/ko-kr/102195
22 https://safety.google/intl/ko/authentication/passkey/

2-3. 활성 세션, 사용 기록 파악하고 관리하기

비밀번호나 2단계 인증, 혹은 패스키 등의 인증을 통과하여 계정이 '인증'되면, '인증'이 끝날 때까지(예를 들어, 로그아웃할 때까지) '인증'한 기기에 로그인 상태가 유지됩니다. 이렇게 로그인되어 있는 상황을 '활성 세션'이라고 합니다. 새로운 활성 세션이 만들어지는 과정을 모니터링하면 자신이 로그인하지 않았음에도 활성 세션이 만들어졌을 경우 계정의 인증 수단이 유출되었음을 알 수 있습니다.

만일 하나의 계정을 여러 사람이 공유하는 경우라면 활성 세션이 만들어졌을 때 계정을 공유하는 사람 중 누가 활성 세션을 만들었는지를 즉시 알 수 있어야 합니다. 만일 계정을 공유하고 있는 사람이 아닌 사람이 활성 세션을 만든 상황이라면 즉시 해당 계정의 인증 방식에 취약점이 발생했음을 인지하고 조치를 취해야 합니다.

<5-2-4 텔레그램 설정 가이드>에서 텔레그램의 활성 세션에 대한 내용을 다루고 있습니다. 구글, 노션 등의 서비스에 대해서도 활성 세션을 모니터링하는 것이 중요합니다. 가능하다면 자신만의 디지털 보안 대책에 정기적으로 중요한 계정들의 활성 세션을 점검하는 절차를 마련하는 것도 한 가지 방법입니다. 예를 들어 아무리 길어도 1개월에 1회는 이메일, SNS, 메신저 등에 대해 일괄적으로 활성 세션을 모니터링하도록 해야 합니다.

2-3-1. 주요 서비스들의 '활성 세션' 혹은 현재 로그인되어 있는 기기 목록 확인 방법

엑스(구 트위터)

- 다음 주소에서 확인할 수 있습니다.
- https://x.com/settings/sessions 또는 [설정 및 개인정보] → [보안 및 계정 접근 권한] → [앱 및 세션] → [세션]에서 확인할 수 있습니다.

페이스북

- 다음 주소에서 확인할 수 있습니다.
- https://accountscenter.facebook.com/password_and_security/login_activity 또는 [설정 및 개인정보] → [설정] → [계정 센터] → [비밀번호 및 보안] → [로그인한 위치] 에서 확인할 수 있습니다.

인스타그램

- 다음 주소에서 확인할 수 있습니다.
- https://accountscenter.instagram.com/password_and_security/login_activity/ 또는 [설정 및 개인정보] → [설정] → [계정 센터] → [비밀번호 및 보안] → [로그인한 위치] 에서 확인할 수 있습니다.

구글

- 다음 주소에서 확인할 수 있습니다.
- https://myaccount.google.com/device-activity 또는 [내 계정] → [보안] → [내 기기] → [모든 기기 관리] 에서 확인할 수 있습니다.

애플

- 다음 주소에서 확인할 수 있습니다.
- https://account.apple.com/account/manage/section/devices

  또는 [Apple 계정] → [기기] 에서 확인할 수 있습니다.

노션

- [설정] → [내 계정] → [기기] 에서 확인할 수 있습니다.

텔레그램

- [설정] → [개인정보 및 보안] → [기기들] → [활성 세션] 에서 확인할 수 있습니다.

3. 악성 코드와 해킹에 대한 이해

3-1. 해킹, 탈옥, 사회공학적 해킹의 이해

3-1-1. 넓은 의미의 해킹

해킹(Hacking)이라는 말을 들으면, 한국에서는 굉장히 강한 어감으로 받아들여지곤 합니다. 엄청난 전문가들만 할 수 있는 굉장한 공격 기술을 일컫는 말처럼 받아들여지곤 합니다. 해킹 피해가 일어났다는 표현이 굉장히 큰 일이 일어난 것처럼 받아들여집니다.

넓은 의미에서 해킹이라고 하는 단어는 정당한 권한이 없이 접근하는 행위 전반을 이야기할 때 쓰는 말입니다. 이를테면 같은 공간에서 거주하고 있는 동거인의 스마트폰에 저장돼 있는 내용을, 그 동거인이 자는 동안에 몰래 지문을 찍어서 보는 상황을 생각해 보겠습니다. 이런 것도 넓은 의미로는 허락을 받지 않고 본 것이기 때문에 해킹이라고 볼 수 있습니다.

3-1-2. 좁은 의미의 해킹

좁은 의미의 해킹은 악성코드나 보안 취약점을 특수하게 이용해서 권한이 없는 컴퓨터나 디지털 기기의 접근 권한을 확보해 내고 권한이 없는 파일의 내용을 유출하거나 파일을 위조, 변조하는 등의 행위를 일컫습니다.

3-1-3. 사회공학적 해킹

악성 코드를 공격 대상의 기기에 설치하기 위해 다양한 수단이 사용됩니다. 이른바 '사회공학적 해킹'(Social Engineering Hacking)이란 사람의 심리적 취약점 등 사람의 특성을 노리고 정보를

유출하거나 조작하는 방법을 말합니다.[23]

23 https://nordvpn.com/ko/blog/social-engineering-attack-types/

3-2. 악성 코드의 유형과 대처법

다른 사람의 컴퓨터에 몰래 들어가거나 악성 코드를 설치하는 것은 더 이상 범죄자 혹은 악의를 가진 해커만의 전유물이 아니게 되었습니다. 정보기관이나 수사기관 또한 스파이웨어 등의 악성 코드를 통해 누군가의 컴퓨터를 몰래 수색하거나 감시하는 것이 확인되고 있습니다.

2015년 7월 6일, 이탈리아의 스파이웨어 개발업체 '해킹팀'이 해킹되어 내부 자료가 유출된 바 있습니다. 해킹팀은 전 세계 정보기관에 RCS라 불리는 스파이웨어를 판매해 온 업체였고, 유출된 자료를 통해 한국의 국가정보원도 RCS 구매처에 포함되어 있음이 알려졌습니다. 대통령 선거가 있었던 2012년에 국가정보원이 해킹팀의 스파이웨어를 구매했고, 이후 계속적인 업그레이드를 요청한 정황이 드러난 것입니다.

악성 코드에 어떤 유형들이 있고, 어떤 대처법이 있는지 살펴봅시다.

3-2-1. 멀웨어(Malware)

일반적으로 악성 소프트웨어(Malicious Software)를 줄여서 멀웨어(Malware)라고 부릅니다. 디지털 기기에 해를 끼치는 프로그램 전반을 일컫는 말입니다. 멀웨어마다 다종다양한 방식으로 컴퓨터에 해를 끼치거나 디지털 보안 공격을 가할 수 있습니다.

운영 체제(OS)를 망가뜨리거나, 민감한 정보를 수집하거나, 설치된 기기의 소유자를 감시하거나, 설치된 기기의 소유자를 사칭하여 스팸 메시지 혹은 조작된 메시지를 보내거나, 보안을 뚫고

침입하게 하는 등 다양한 유형의 악성 코드가 존재합니다.

이러한 악성 코드를 유포하는 주체가 과거 특수한 해킹 전문 기술을 갖고 있는 사람들이나 범죄자에 국한되었다면, 현대에는 민간인을 사찰하고 감시하고자 하는 정부 기관이나 법 집행기관(수사기관)은 물론 그저 시간이 많은 개인이나 10대 청소년들까지도 확장되고 있는 추세입니다.

3-2-2. 스파이웨어(Spyware)

기기의 카메라나 마이크를 사용하여 영상을 촬영하기도 하고, 기기에 입력되는 사용자의 비밀번호를 가로채는 등의 행위를 하는 악성 코드를 스파이웨어라고 부릅니다.

스파이웨어를 비롯한 악성 코드 공격에 대처하는 가장 좋은 방법은 처음부터 감염되지 않는 것입니다. 즉 악성코드를 설치하지 않는 것입니다. 대부분의 현대적인 디지털 기기는 사용자가 특정한 행위를 하지 않는 한 어떤 프로그램도 자동으로 설치하기 어렵기 때문입니다. 따라서 공격자가 여러분이 직접 악성코드를 설치하도록 속이는 방법이 일반적입니다.

공격자가 여러분의 컴퓨터에 악성코드를 설치하도록 속이는 방법은 여러 가지가 있습니다. 악성코드가 포함된 파일을 웹사이트 링크, 문서, PDF 파일 또는 심지어 컴퓨터 보호 프로그램으로 위장할 수 있습니다. 여러분은 이메일이나 문자 메시지, 혹은 메신저 메시지를 통해 표적이 될 수 있으며, 여러분이 받은 메시지는 여러분이 잘 아는 사람으로부터 온 것처럼 보일 수 있습니다. 카카오톡, 텔레그램 등의 메신저, 혹은 페이스북과 같은 SNS 페이지에 게시된 링크를 경유할 수도 있습니다.

3-2-3. 제로데이 공격(Zero-day Attack)과 제로클릭 원격 코드 실행(Zero-Click Remote Code Execution)

공격자가 제로데이 취약점을 사용할 수 있다면, 즉 제로데이 공격을 할 수 있다면 이러한 다양한 멀웨어의 감염을 피하기가 어려울 수 있습니다. 제로데이 공격은 해당 공격이 발견된 시점까지 파훼법이 알려지지 않은 취약점을 이용한 공격을 통칭하는 말입니다. 제로데이 공격이 실제로 관찰되어 해당 보안 취약점을 가진 앱, 프로그램, 운영체제 등에 보안 업데이트가 이뤄지면, 사용자는 이러한 보안 업데이트를 자신의 기기에 실제로 적용함으로써 해당 공격으로부터 안전해질 수 있습니다. 하지만 파훼법 자체가 마련되지 못한 상황이 이어지는 경우, 혹은 사용자가 자신의 기기에 보안 업데이트를 진행하지 않는 경우 등 다양한 이유로 제로데이 공격은 큰 피해를 야기할 수 있습니다.

제로데이 공격이면서 동시에 제로클릭 원격 코드 실행 취약점인 경우에는 더더욱 문제가 심각해집니다. 예를 들어 2023년 발견된 BLASTPASS 사건의 경우, iOS 16.6 및 그 이하 버전을 사용하는 사람들이 특수한 메시지를 '받기만 해도', 즉 기기에 메시지가 수신이 되기만 해도 악성 코드가 자동으로 실행되는 보안 취약점을 이용한 공격이었습니다.[24] 이 공격은 발견된 이후 애플의 iOS 16.6.1 보안 업데이트를 통해 차단되었지만, 보안 업데이트를 실행하지 않고 iOS 16.6 기기를 사용하는 사람들은 여전히 공격 대상으로 남았습니다. 제로클릭 원격 코드 실행 취약점의 특성상 자신이 공격받았는지의 여부를 알기 어렵고, 또한 제로데이 공격이기 때문에 보안 업데이트를 진행하지 않고서는 공격

24 https://www.mallocprivacy.com/blog/the-blastpass-incident/ https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/

대상으로 남는 특성 때문에 더욱 큰 피해를 입힐 수 있었습니다.

정부와 법 집행 기관은 표적형 악성코드 공격에 사용할 수 있도록 제로데이 취약점을 비축해 둡니다. 물론, 범죄자나 다른 공격자들도 제로데이 취약점을 사용해 악성코드를 은밀히 설치할 수 있습니다. 그러나 제로데이 취약점은 보통 알아내기까지 드는 비용도 크고 재사용이 어려울 가능성이 큽니다. 한 번이라도 제대로 사용된 취약점은 다른 사람들이 그 취약점을 발견할 가능성이 그만큼 커지고, 이로 인해 해당 취약점 관련 조치가 취해질 것이기 때문입니다.

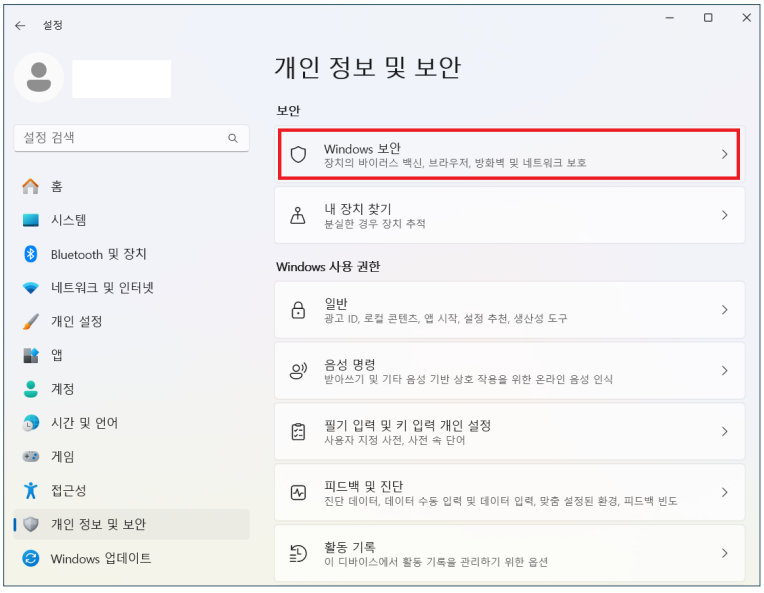
3-2-4. 랜섬웨어(Ransomware)

악성 코드 중 컴퓨터에 저장된 정보를 이상한 방식으로 암호화하고는 데이터를 살리고 싶다면 돈을 내라고 협박하는 유형의 악성 코드를 랜섬웨어(Ransom + ware)라고 합니다.

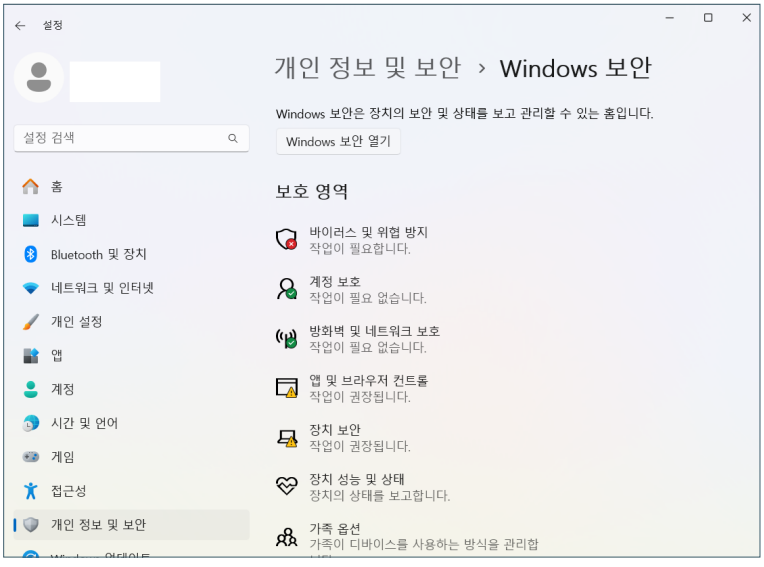
3-2-5. 백신(Antivirus) 사용 및 백신의 한계

불특정 다수를 상대로 한 공격에 사용되는 악성 코드를 방어하기 위해 백신(Antivirus) 프로그램의 사용은 선택이 아닌 필수입니다. 현대의 운영 체제들은 운영체제 공급사의 최신 보안 업데이트를 적용하는 것이 무엇보다 선행되어야 할 일입니다. 윈도우를 사용하는 경우, 다른 백신 프로그램을 설치하지 않았다면 윈도우에 기본 내장된 윈도우 보안(Windows 보안)을 활성화하는 것도 한 가지 방안입니다.

윈도우 보안이 활성화되어 있는지를 알고 싶다면, 윈도우의 [설정]에서 [개인 정보 및 보안]의 [Windows 보안]으로 들어가서 확인할 수 있습니다.



[개인 정보 및 보안] → [Windows 보안] 화면까지 넘어오면,
여기서 [Windows 보안 열기]로 들어갑니다.



이제 [Windows 보안]의 [보안 한 눈에 보기] 화면에서, [바이러스 및 위협 방지]가 꺼져 있다면 여기서 [켜기]를 선택합니다.

리눅스나 맥 사용자의 경우 ClamAV[25] 같은 멀웨어 탐색 도구를 사용하는 것도 좋습니다. 시스템을 실시간으로 모니터링하며 멀웨어에 대한 감염 자체를 예방하는 역할을 하지는 못하지만, 최소한 현 시점에 잘 알려진 악성 코드가 설치되어 있는지의 여부를 판단하는 데에는 도움이 됩니다.

백신을 비롯한 악성 코드 감염 차단 모니터링 목적의 보안 도구들의 우열을 가리는 것은 몹시 어려운 일입니다. 개개인이 처한 상황, 새로운 악성 코드의 출현 등 너무나 다양한 변수가 있기 때문입니다. 따라서 특정한 악성 코드 감염 차단 혹은 감염 여부 확인 도구 하나에 의존하기보다는, 큰 수고 없이 활성화할 수 있는 예방책을 활성화하는 것에 의의를 두는 것이 좋습니다.

또한 불특정 다수를 상대로 한 공격이 아닌 맞춤형 공격이 가해지고 있는 경우, 대중적인 백신 프로그램이 이를 방어하는 데 효과적이지 않을 수도 있습니다.

3-2-6. 최신 보안 업데이트 유지

윈도우, 리눅스, 맥, 안드로이드, iOS 등 어떤 운영체제를 사용하더라도 운영체제 자체의 최신 보안 업데이트를 유지하는 것이 최선입니다. 사용중인 운영체제의 최신 보안 업데이트가 있는지 주기적으로 살피고, 보안 업데이트를 설치하세요. 운영체제뿐만 아니라 주요 앱의 경우에도 가능한 최신 업데이트 상태를 유지하는 것이 중요합니다.

25 https://www.clamav.net/

3-2-7. 웹 브라우저 스크립트 실행 차단 고려

웹사이트를 통한 악성 코드 설치를 원천 봉쇄하는 방법은 사용중인 웹 브라우저가 기본적으로 어떤 종류이든 '스크립트'를 실행하지 않고 오직 당신이 신뢰하는 웹 사이트에 대해서만 '스크립트'를 실행하도록 하는 확장 프로그램을 사용하는 것입니다. NoScript[26] 같은 확장 프로그램을 사용하는 것이 한 가지 방법입니다.

3-2-8. 악성 코드 감염 여부 자가진단 및 물리적 보안 조치

웹캠이 내장되어 있는 노트북, 혹은 전면 카메라가 내장되어 있는 스마트폰 대부분은 웹캠이나 전면 카메라가 작동할 때 카메라 우측에 녹색 불이 켜지도록 설계되어 있습니다. 카메라를 활성화한 적이 없는데 이런 상황이 발견될 경우 악성 코드에 감염된 상황을 의심할 수 있습니다.

혹은 이메일 설정이 변경되었는지의 여부를 확인해볼 수 있습니다. '보낸 편지함'에 내가 보낸 적이 없는 이메일이 있고, 특히 이러한 이메일을 나의 이메일 주소가 아닌 다른 이메일 주소를 사용하여 보내도록 설정되어 있는 상황이 발견되면 악성 코드 감염 혹은 다른 형태의 디지털 보안 문제가 발생했다는 지표가 될 수 있습니다.

만일 네트워크 트래픽을 모니터링하고 있다면(내 컴퓨터나 스마트폰 등이 어떤 웹사이트나 서버에 언제 접속하여 어느 정도 분량의 데이터를 주고받는지), 평소와 다른 네트워크 트래픽이 발생했는지의 여부를 통해 악성 코드 감염의 징후를 발견할 수도 있습니다.

---

26 https://noscript.net/

3-2-9. 이미 멀웨어에 감염되었다면

일부러 당신을 노리고 고도로 정교한 공격이 가해지고 있는 상황에서는, 당신이 열어볼 수밖에 없는 문서 형태의 첨부파일로 위장한 악성 코드를 당신이 직접 열어서 당신의 컴퓨터나 스마트폰 등의 디지털 기기가 감염되는 일을 피하기 어려울 수 있습니다. 그렇게 어쩔 수 없이 멀웨어에 감염된 상황을 확인하면 어떤 조치를 취해야 할까요?

가장 급선무는 컴퓨터나 스마트폰 등의 기기와 인터넷의 연결을 끊는 것입니다. 이더넷(랜선), 와이파이 뿐만 아니라 블루투스, 모바일 데이터 등 모든 종류의 네트워크 연결을 끊는 게 최선책입니다. 그리고 믿을 수 있는 디지털 보안 전문가에게 감염된 기기를 맡겨야 합니다. 단순히 멀웨어를 삭제하는 프로그램을 사용하고, 멀웨어가 삭제된 것처럼 느껴지는 것만으로는 안전을 보장할 수 없습니다. 멀웨어가 확산되는 것을 막기 위해 USB 메모리나 외장 하드 드라이브의 연결도 삼가야 합니다.

안전하다고 믿을 수 있는 컴퓨터를 확보하고, 그 컴퓨터에서 각종 계정에 로그인하여 비밀번호를 변경해야 합니다. 비밀번호 관리 도구를 사용중이라면 비밀번호 관리 도구의 마스터 패스워드도 변경해야 합니다.

4. 파일과 기기, 운영체제의 보안

4-1. 파일과 저장기기

4-1-1. 항상 파일을 암호화해서 저장해야 하는 이유

공격자로부터 당신의 데이터를 보호하는데 있어서 가장 큰 난관 중 하나는 당신이 보관하고 있는 정보 자체가 많다는 것과 그것을 훔치는 것이 상당히 쉽다는 것에 있습니다. 과거의 연락처, 통신 내용, 현재의 문서들이 노트북이나 스마트폰에 저장되어 있습니다. 개중에는 수십, 수천 명에 이르는 사람들의 민감한 정보가 담겨있기도 합니다. 스마트폰이나 노트북이 도난당하거나 압수당하면 그 안에 있던 데이터가 순식간에 복제될 수 있습니다. 이런 일이 발생할 가능성을 염두에 두고, 데이터를 항상 암호화하여 저장해 둘 수 있어야 합니다.

보안 메신저를 사용하는 등의 방법을 써서 통신 내용을 암호화하여 더 안전하게 소통하는 것과 마찬가지로, 데이터 또한 좀더 안전하게 저장하기 위해서는 데이터 자체가 저장되어 있을 때 암호화된 채로 저장되어 있도록 해야 합니다. 화면 '잠금'조차 설정되어 있지 않은 기기라면 압수당했을 때 데이터가 쉽게 읽을 수 있는 방법으로 저장되어 있기 때문에, 아직 스마트폰의 화면 '잠금'을 설정하지 않았다면 지금 즉시 잠금을 설정해야 합니다. 화면 '잠금'기능과 데이터 암호화가 직결되기 때문입니다. 구체적인 내용은 <4-3 스마트폰 자체의 보안>을 참고하세요.

스마트폰의 화면 '잠금'과 별개로 데이터 자체를 암호화하여 저장하는 것도 중요합니다. USB 메모리나 외장 하드디스크 등에 데이터가 암호화되지 않은 채로 저장되어 있다면 데이터가 그만큼 간편하게 유출될 것이기 때문입니다. 몇 개의 폴더만이 아니라, 당신의

데이터 전체를 암호화하는 것이 가장 안전하고 단순합니다.

윈도우를 사용하는 컴퓨터에는 모든 데이터를 암호화하여 저장하는 '비트로커(BitLocker)'가 기본으로 제공됩니다. 애플의 OS X에서는 내장된 '파일볼트(FileVault)'를 이용할 수 있습니다. 만일 여러 OS를 사용한다면 베라크립트(VeraCrypt)와 같은 프로그램을 사용하여 여러 OS에서 동시에 공유할 수 있는 암호화 방식으로 데이터를 암호화하여 저장하는 것을 고려할 수 있습니다.

이렇게 암호화된 데이터도 무차별 대입 공격 시도를 통해 복호화를 시도하는 공격자의 노력 앞에서 무너질 수 있습니다. 아주 단순한 비밀번호를 사용하여 암호화한다면 무차별 대입 공격 시도 앞에서 금방 무너진다는 점에 유의해야 합니다. 그렇다고 스마트폰 잠금화면의 비밀번호를 일상적으로 매우 긴 비밀번호로 유지하기도 어렵기 때문에, 절대로 유출되어서는 안 되는 기밀 데이터는 처음부터 공격자가 물리적으로 접근할 수 없는 곳에만 보관하는 방법을 취하거나, 보안성이 훨씬 안전한 기기를 사용하여 접근을 통제해야 합니다.

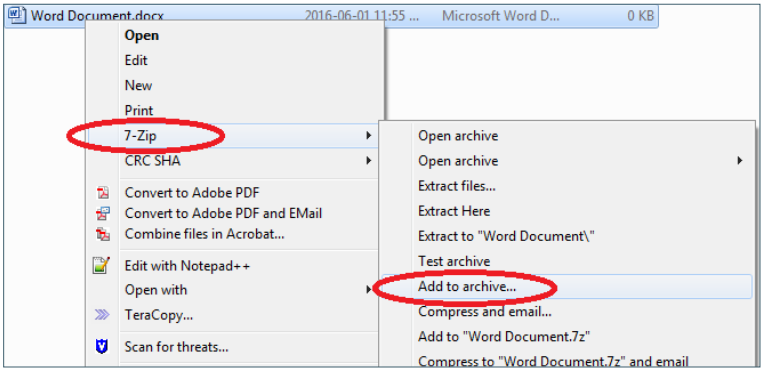
윈도우에서 7-Zip 을 이용한 파일 암호화

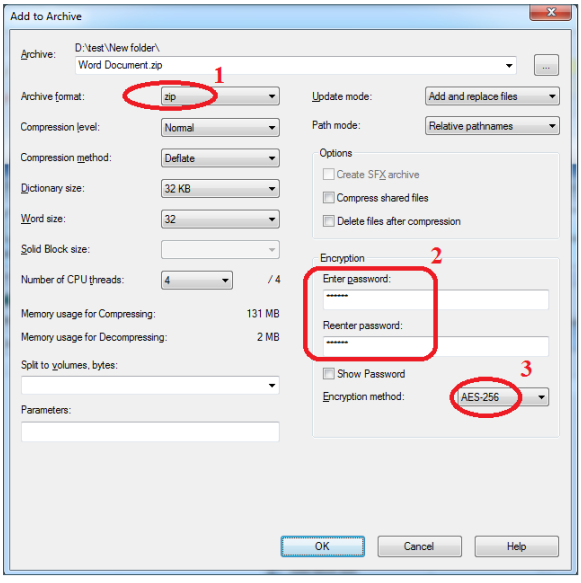
7-Zip은 여러 개의 파일이나 폴더를 하나의 압축 파일로 묶거나, 혹은 파일의 압축을 해제할 수 있는 자유, 오픈 소스 소프트웨어입니다.[27] 윈도우에 기본 내장되어 있는 파일 압축 기능은 비밀번호를 이용한 암호화를 지원하지 않지만, 파일 압축 해제 기능은 복호화를 지원합니다. 따라서 7-Zip을 이용하여 zip 형식으로 파일을 압축하면서 암호를 지정하면, 비밀번호를 알고 있는 사람은 7-Zip이 없더라도

27 https://www.7-zip.org/

윈도우에서 그 압축 파일의 내용을 열어볼 수 있게 됩니다.

7-Zip을 설치하고, 아래 사진의 절차에 따라 비밀번호를 설정하세요.
먼저, 암호화하고자 하는 파일을 탐색기나 '내 컴퓨터', '바탕화면'등에서 선택한 다음 마우스 오른쪽 버튼을 클릭합니다. 여기서 [7-Zip]에 마우스 커서를 올려 나오는 메뉴 중 [Add to archive...]를 선택합니다. 그러면 7-Zip의 [Add to Archive] 창이 열립니다.





열린 창에서 [Archive format]은 [zip]을 선택합니다. 7-Zip이 설치되어 있지 않더라도 대부분의 윈도우, 맥, 리눅스 등에서 zip 형식을 지원합니다. 창의 오른쪽 하단에 [Encryption] 영역에서 [Enter password], [Reenter password]에 암호화 및 복호화에 사용될 비밀번호를 입력합니다. Encryption method는 기본값을 그대로 사용합니다. 이제 [OK]단추를 클릭하면 해당 비밀번호를 사용하여 암호화된 압축 파일이 생성됩니다.

비밀번호는 본질적으로 다른 사람이 '몰라야' 하는 정보이므로, 편의성을 위해 압축 파일의 이름에 비밀번호를 적는 것은 곤란합니다. 파일 이름만 보면 비밀번호를 알 수 있다면 다른 사람이 '모를 수 없는' 정보가 되기 때문입니다. 암호화된 파일을 복호화하는 비밀번호는 제3의 경로로 전달하세요. 예를 들어 암호화된 첨부파일을 이메일로 보내고, 비밀번호는 전화를 통해 전달하는 방법을 생각할 수 있습니다. 이렇게 되면 설령 이메일과 함께 암호화된 첨부파일이 유출되더라도 전화통화까지 도청하지 않고서는 비밀번호를 알아낼 수 없어, 공격자로 하여금 공격을 어렵게 만들 수 있습니다.

4-1-2. 보안 전용 컴퓨터 별도 운용하기

자료가 유출되지 않는 안전한 환경을 유지하는 것은 어려운 일입니다. 디지털 보안 대책을 정기적으로 점검하더라도 비밀번호와 관련된 정책을 변경하거나, 컴퓨터나 기기에서 사용하는 소프트웨어를 변경하는 수준에서 머무를 수도 있습니다. 최악의 경우 자기도 모르는 사이에 기밀 정보를 유출하고 있지는 않은지, 실질적으로는 전혀 안전하지 않은 디지털 보안 대책의 절차를 기계적으로 관성적으로 유지하고 있는 것은 아닌지를 고민해야 할 수도 있습니다.

<현 시점의 '우리 편'과 의논할 사항은?>에서도 다뤘지만, 디지털 보안 위험을 설명하더라도 함께 일하는 동료들이 안전하지 않은 디지털 보안 관행을 요구할 수도 있습니다. 예를 들어, 동료 활동가들이 업무 효율성을 위해 당신에게 자신이 보낸 이메일 첨부파일을 가급적 빠르게 즉시 열어보기를 요청할 수도 있습니다. 그러나 그러한 요청은 공격자들이 당신의 동료로 가장해서 악성 소프트웨어를 보낼 경우 바로 악성 코드 감염을 일으키는 원흉이 됩니다.

이러한 상황에서 고려할 수 있는 한 가지 방법은, 좀더 안전한 컴퓨터에만 보안성이 높은 데이터나 통신기록을 보관하고 접근을 통제하는 것입니다. 그 컴퓨터는 단지 가끔씩만 사용하고, 사용할 때에는 훨씬 더 많은 주의를 기울여야 합니다. 이를테면 첨부 파일을 열 필요가 있거나 안전하지 않은 소프트웨어를 이용할 때에는 그 컴퓨터를 사용하지 않도록 해야 합니다. 즉, 첨부 파일을 열고 안전성을 검토하는 작업을 할 때에는 이렇게 설정한 '보안 전용 컴퓨터'가 아닌 별도의 컴퓨터가 필요합니다.

'보안 전용 컴퓨터'를 별도로 마련하는 것이 너무 어렵다면, 테일즈(Tails)와 같이 프라이버시 및 보안에 초점을 둔 운영체제를 사용하는 것도 고려해볼 수 있습니다.[28] 일상적인 업무가 아닌, 민감한 이메일을 주고받는 활동이나 보안이 민감한 파일을 열람하는 수준의 활동을 할 때, 혹은 포렌식 등으로부터 안전한 작업을 할 필요가 있을 때에는 테일즈(Tails) OS가 설치된 USB메모리를 이용하여 컴퓨터를 부팅시키고, 높은 보안 설정을 기본값으로 하여 사용하는 방식을 고려해볼 수 있습니다.

일상적인 업무용 컴퓨터와 별개로 보안 전용 컴퓨터를 운용하는 데는

28 https://tails.net/

그리 많은 비용이 들지 않을 수 있습니다. 보안 전용 컴퓨터라는 목적으로는 반드시 최신 노트북을 사용할 필요도 없고, 중고 노트북에서 충분히 많은 작업을 할 수 있습니다.

4-1-3. 단일 공격 목표 만들지 않기

높은 기밀성이 필요한 데이터를 보관하기 위해 보안 전용 컴퓨터를 별도로 운용할 경우, 이에 따른 추가적인 위험 요소를 고려해야 합니다. 당신의 소중한 정보를 하나의 컴퓨터에 집중시키면, 이 사실을 알게 된 공격자는 그 '보안 전용 컴퓨터'를 단일 공격 목표로 지정하고 오직 그 컴퓨터를 노리기 위해 움직일 수도 있습니다. 이러한 민감한 데이터가 보관되어 있는 '보안 전용 컴퓨터'는 그 위치를 가능한 한 숨겨야 하고, 강력한 암호로 드라이브를 암호화하는 것을 잊지 말아야 합니다. 설령 도난당하더라도 비밀번호 없이는 데이터를 읽을 수 없는 상황을 보장해야 합니다.

동시에, 이 하나의 기기를 파괴하면 그 데이터가 복구 불가능하게 파괴될 위험성을 만들 가능성이 있습니다. 공격자는 이러한 데이터가 보존되어 있는 컴퓨터에 대해 랜섬웨어를 심기 위한 공격을 펼쳐올 수도 있습니다. 어떤 식으로든 공격자가 당신의 모든 데이터를 없애는 것으로부터 이익을 얻는다면, 아무리 안전하더라도 데이터를 단 하나의 장소에만 보관하면 곤란합니다. 데이터의 백업 복제본을 암호화하여 또 다른 공간에 보관하는 것이 필요합니다.

4-1-4. 물리적으로 격리된 환경 유지하기

인터넷 공격이나 온라인 감시로부터의 가장 높은 수준의 보안을 달성하는 방법은 당연히 인터넷에 연결하지 않는 것입니다. 당신의 보안 전용 컴퓨터를

절대 네트워크나 와이파이에 연결하지 않아야 한다는 말입니다. 데이터를 옮길 때는 네트워크를 사용하지 말고 DVD나 USB 디스크와 같은 물리적인 매체를 이용해 그 컴퓨터에 복제해야 합니다. 네트워크 보안에서 이는 컴퓨터와 세계 사이의 '공간 격리(air gap)'라고 표현합니다. 데이터를 거의 접근할 수 없는 상태로 보관하면서 도난당하고 싶지 않다면, 이 정도 수준의 물리적인 격리는 충분히 고려할 가치가 있습니다. 예를 들어, 당신이 중요한 메시지를 위해서만 사용하는 암호키, 비밀번호 목록이나 당신이 없을 경우 다른 사람이 알아야 할 지시 사항, 혹은 당신에게 맡겨진 다른 사람의 사적인 데이터의 백업 복제본 등은 이렇게까지 공들여 물리적으로 격리할 만한 가치가 있습니다. 컴퓨터 전체를 격리하는 것도 좋은 방법이지만, 저장기기만 격리하는 것도 고려해 볼 수 있습니다.

4-1-5. 논리적으로 격리된 환경 유지하기

보안 전용 컴퓨터를 굳이 인터넷에 연결해야만 하는 경우, 당신이 일상적인 업무에서 사용하는 계정을 사용하거나 로그인하거나 하는 행위를 해서는 곤란합니다. 보안 전용 컴퓨터에서의 통신에 사용하는 별개의 웹 계정이나 이메일 계정을 만들고, IP 주소를 감추기 위해 토르(Tor)를 사용하는 등의 방법을 써서, 각각의 컴퓨터에서 이뤄지는 행위가 논리적으로 분리되도록 해야 합니다.

4-1-6. 보안 위험 컴퓨터 별도 운용하기

보안 전용 컴퓨터를 별도로 운용하는 아이디어를 살짝 비틀어서 안전하지 않은 작업을 할 때에만 사용하는 컴퓨터를 별도로 운용하는 것도 한 가지 방법입니다. 즉, 위험한 지역에 가거나 혹은 보안 위협에 노출될 수 있는 작업을 할 때에만 특정 장비를 사용하는 것입니다. 분실하거나 공격자에게

노출되더라도 문제가 될 만한 정보가 전혀 들어있지 않은 별도의 기기를 사용하는 것이 디지털 보안을 유지하는 좋은 방법이 될 수 있습니다.

4-1-7. 파일을 안전하게 삭제하려면

클라우드 공간에 저장된 데이터를 복구가 불가능한 방법으로 삭제할 수 있는 방법은 보장되지 않습니다. 복구가 불가능한 형태로 파일의 삭제가 완전히 이뤄져야 하는 상황이 필요하다면, 클라우드 공간에 데이터를 저장해서는 안 됩니다. 네트워크를 통해 누군가에게 전송된 적이 있는 파일은 완전히 삭제하는 것이 불가능할 수 있다는 점을 잊어서는 안 됩니다.

하드디스크, SSD 등 저장장치에 따라 시도해볼 수 있는 파일의 완전한 삭제 방법은 2015년도의 디지털 보안 가이드의 <데이터의 안전한 보호 및 삭제>를 참고하세요.[29] 핵심적인 내용은 "저장장치 자체를 물리적으로 파괴할 수 있다면 가능한 한 물리적으로 산산조각내어 파괴해야 한다"는 것과, 저장장치의 수명을 늘리기 위한 기술로 인해 발생하는 한계를 극복하기 위해 "저장장치의 모든 공간을 쓰레기 데이터로 가득 채우고 삭제하는 작업을 수 차례 반복"해야 한다는 점입니다. 스마트폰의 경우에도 2015년의 디지털 보안 가이드의 <휴대전화 데이터의 안전한 보호 및 삭제>를 참고하세요.[30] 현실적으로 파일의 완전한 삭제를 보장하려면 처음부터 파일이 언제나 암호화된 형태로 저장되어, 애초에 파일이 원본 그대로 복원될 가능성 자체를 낮춰야 한다는 것을 명심하세요.

---

29 https://guide.jinbo.net/digital-security/computer-security/safe-deletion-data
30 https://guide.jinbo.net/digital-security/smartphone-security/safe-deletion-smartphone-data

4-2. 컴퓨터 운영체제의 보안

4-2-1. 윈도우(Windows) 보안의 기초

한국의 인터넷 환경은 인터넷 금융, 공공기관(정부기관) 관련 작업을 할 때 무수히 많은 디지털 보안 취약점 투성이가 되는 것으로 유명합니다. 2023년 1월 2일부터 독일의 Wladimir Palant는 <South Korea's online security dead end>라는 글을 통해 한국의 인터넷 금융, 공공기관(정부기관) 관련 작업을 할 때 의무적으로 설치하게 되는 프로그램들이 다종다양한 보안 취약점을 갖고 있음을 여섯 차례에 걸쳐 발표했습니다.[31]

구체적인 동작원리나 문제점을 알지 못한 채로 정부기관에서 Active-X에 대한 '묻지마 설치'를 강요하는 보안 방식때문에 한국의 인터넷 환경이 위험해졌다는 지적은 자주 있어왔습니다.[32] Active-X 라는 특정 방식에서 벗어나기는 했지만 여전히 한국에서는 '보안 프로그램'을 설치하지 않으면 업무 자체가 불가능한 상황을 자주 만나게 됩니다.
이런 '보안 프로그램'들이 실제로는 보안 취약점을 만드는 경우가 많다는 것이 문제의 핵심이고, 따라서 디지털 보안을 위해서는 정부기관 등의 요구에 따라 어쩔 수 없이 아주 특수한 '보안 프로그램'을 설치해야 하는 업무는 별도의 기기(PC)에서 진행하는 것이 바람직합니다.

---

31 https://palant.info/2023/01/02/south-koreas-online-security-dead-end/
https://docs.woojinkim.org/wiki/spaces/me/pages/733085820/South+Korea+s+online+security+dead+end
https://github.com/alanleedev/KoreaSecurityApps/blob/main/01_touchen_nxkey.md
32 https://act.jinbo.net/wp/wp-content/uploads/2013/05/20130430%EA%B8%B0%EC%9E%90%EA%B0%84%EB%8B%B4%ED%9A%8C_%EA%B8%88%EC%9C%B5%EC%95%B1.pdf

이외에 윈도우 보안에서 특별히 신경써야 하는 지점들은 다음과 같습니다.

Microsoft Copilot 등 기본 내장 생성형 AI 서비스 비활성화에 대한 판단

윈도우 11부터 생성형 AI 기술인 Microsoft Copilot이 윈도우에 기본적으로 내장되었습니다.[33] 생성형 AI는 특정한 조건에서 업무 생산성을 강화하고 이전까지 못 하던 다양한 일을 빠른 시간에 해낼 수 있도록 도와주지만, 그 과정에서 많은 경우 생성형 AI 서비스 운영 기업에게 다양한 정보가 전달됩니다. 특히 윈도우 자체에 기본적으로 내장되는 Copilot은 예상치 못한 상황에서 생성형 AI 서비스를 통해 외부로 전송되면 안 되는 정보가 전송되는 상황을 초래할 수 있습니다. 따라서 Microsoft Copilot 등의 기본 내장된 생성형 AI 기술을 사용하지 않도록 설정하는 방안을 고려해볼 수 있습니다.[34] 구체적인 방법은 시간이 지나면서 조금씩 변화하므로, 'How to disable Microsoft Copilot'같은 검색어를 사용하여 비활성화하는 방법을 찾아보고 적용하세요.[35]

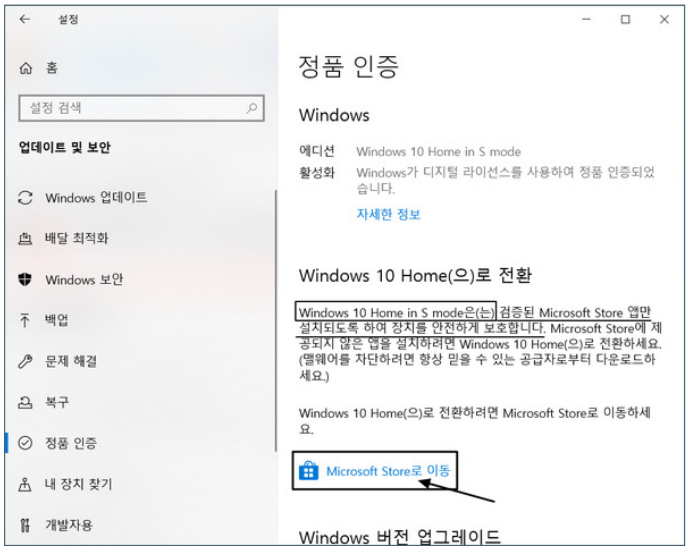
'Windows에서 S Mode 에서 전환'에 대한 판단

윈도우 11 부터 마이크로소프트는 Microsoft Store에 등록된 프로그램만 설치할 수 있도록 하는 윈도우 11 S Mode를 공급하고 있습니다.[36] 이는 마이크로소프트가 윈도우에서 실행될 수 있는 프로그램들을 직접 인증하고 위험성이 없는 프로그램만 설치될 수 있도록 하겠다는 방향성을 시사하지만, 동시에 디지털 보안 가이드북에서

33 https://www.microsoft.com/ko-kr/windows/copilot-ai-features
34 https://www.theverge.com/2024/6/3/24170305/microsoft-windows-recall-ai-screenshots-security-privacy-issues
35 https://answers.microsoft.com/en-us/windows/forum/all/how-do-i-disable-copilot-and-all-other-ai/e74a841f-794c-48d2-9a8a-e3ccfac8ea86
36 https://support.microsoft.com/ko-kr/windows/windows%EC%97%90%EC%84%9C-s-%EB%AA%A8%EB%93%9C%EC%97%90%EC%84%9C-%EC%A0%84%ED%99%98-4f56d9be-99ec-6983-119f-031bfb28a307

과거 다뤄진 많은 보안 프로그램들 중 Microsoft Store에 등록되지 않은 프로그램은 사용할 수 없게 된다는 것을 뜻하기도 합니다.

이러한 이유로 원활한 업무를 하는 것이 불가능한 경우, “Windows에서 S Mode 에서 전환”(하여 Windows 11 Home 등으로 전환)을 고려해볼 수 있습니다.



4-2-2. 리눅스 보안의 기초

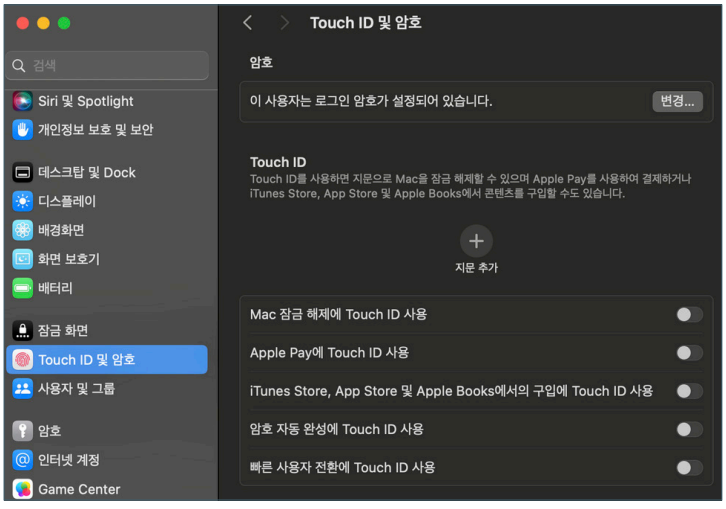
한국에서는 아직 개인 또는 시민단체의 업무용 목적으로 리눅스를 사용하는 경우가 많지 않습니다. 이는 한국에서의 업무 환경에서 리눅스만으로는 어려운 경우가 많기 때문입니다. 그만큼 리눅스 사용자의 경우 윈도우나 맥 사용자와는 달리 처음부터 컴퓨터 사용에 대한 많은 지식을 가진 채 컴퓨터를 사용하게 되는 경우가 많습니다. 그럼에도 이런 지점은 놓치지 말고 꼭 챙겨서 주의해야 합니다.

오픈 소스 공급망 취약점을 노린 악의적 공격에 대한 대처

2021년부터 3년간 리눅스 사용 시 필수적으로 활용되던 오픈 소스 라이브러리에 선의의 기여자 역할을 하면서 대중의 신뢰를 확보한 뒤, 이를 기반으로 2024년에 오픈 소스 라이브러리에 악성 코드를 숨겨 전세계 리눅스 사용자를 공격하려고 한 사례가 발생했습니다.[37] 후일을 도모하기 위해 협조적인 아군 역할을 하는 사례에 당하지 않도록 주의가 필요합니다.

4-2-3. 맥 보안의 기초

생체 인식 비활성화 고려



37 https://m.boannews.com/html/detail.html?idx=128372
https://www.igloo.co.kr/security-information/%EB%8D%B0%EC%9D%B4%ED%84%B0-%EC%95%95%EC%B6%95-%EB%9D%BC%EC%9D%B4%EB%B8%8C%EB%9F%AC%EB%A6%AC-xz-utils-cve-2024-3094-%EB%B6%84%EC%84%9D-%EB%B0%8F-%EB%8C%80%EC%9D%91%EB%B0%A9%EC%95%88/

생체 인증은 편리할 수도 있지만 누군가가 당신의 지문 등을 이용하기
위해 당신을 물리적으로 억압하거나 하여 당신의 맥 컴퓨터에서
정보를 쉽게 확보할 수 있게 하는 수단이 될 수도 있습니다.
이러한 상황에 저항할 수 있는 방법 중 하나는 기본적으로
컴퓨터의 생체 인증을 비활성화하는 것입니다.

4-3. 스마트폰 자체의 보안

4-3-1. 스마트폰이 초래한 보안 위협

스마트폰이 초래한 보안 위협에 대한 전반적인 내용은 2015년 디지털 보안 가이드의 <휴대전화와 관련된 보안 이슈>를 참고하세요.[38]

4-3-2. 안드로이드 보안 설정

안드로이드(Android) 스마트폰은 제조사마다 구체적인 내용이 조금씩 다릅니다. 큰 틀은 Google에서 설계하고 공급하지만 실제 스마트폰에 맞춰서 제조사마다 일부 변형을 가하기 때문입니다. 따라서 아래 내용 중 일부는 스마트폰 제조사에 따라서는 적용하기 어려운 것도 있습니다.

SIM(USIM) 카드 잠금 설정

SIM Swapping(심 스와핑) 등 다른 사람의 휴대전화번호로 전달되었어야 하는 정보를 제3의 기기에 전송받는 보안 위협이 급증하고 있습니다. 이 중에는 남의 휴대폰에서 SIM(USIM)을 몰래 꺼내 다른 스마트폰에 집어넣는 방식도 활개를 치고 있습니다.[39] 이러한 방식에 대응하기 위해서는 SIM 칩 자체에 비밀번호를 설정해야 합니다. 이를 SIM 카드 잠금 설정이라고 합니다. 기본적으로는 설정되어 있지 않고, 설정 이후부터는 휴대전화를 켤 때마다 패턴 등에 더하여 추가로 SIM 비밀번호를 입력해야 하는 불편함이 생기지만 익숙해 질 수 있는 문제이니 필수적으로 설정하세요. 설정 이후에는 누군가 스마트폰에서 몰래 내

38 https://guide.jinbo.net/digital-security/smartphone-security/problem-mobile-phones
39 https://www.sedaily.com/NewsView/260XD7N878

SIM(USIM)을 꺼내 다른 스마트폰에 집어넣어도, 전원을 켰을 때 해당
SIM에 설정된 비밀번호(PIN)를 모르면 USIM을 사용할 수 없습니다.

[설정] → [보안 및 개인정보 보호] → [기타 보안 설정] →
[SIM 카드 잠금 설정] → [USIM 카드 잠금 설정]에서 설정합니다.

화면 잠금 설정

[설정] → [보안 및 개인정보 보호] → [화면 잠금]에 있는 화면
잠금(Screen Lock)은 아예 설정하지 않으면 위험합니다.
화면 잠금 설정이 되어 있어야 최소한의 안드로이드 보안이 작동한다는
점에 유의하세요. PIN, 패턴, 비밀번호 중 적당한 것으로 설정해야 합니다.
단, 패턴의 경우 최근에는 스마트폰 화면에 남아있는 지문
흔적을 보고 알아내는 사례가 있으므로 주의해야 합니다.
또한 너무 길지 않은 시간으로 화면 자동 잠금 시간도 설정합니다.

보안 폴더 사용

삼성 등 특정 스마트폰 제조사는 '보안 폴더' 등의 형태로 몇 가지 앱이나
폴더에 대해 추가적인 암호화를 지원합니다. 스마트폰의 화면 잠금을 풀어도
개별 앱에 대해서는 추가적인 암호를 입력해야만 접근할 수 있기 때문에,
기기를 분실하거나 기기의 화면 잠금이 풀리더라도 특정 앱, 특정 폴더의
내용은 추가적인 암호를 빼앗기기 전까지는 상대적으로 안전할 수 있습니다.

안드로이드의 경우 스마트폰 제조사마다 이러한 기능의
명칭과 동작 방식이 조금씩 다르기 때문에, 구체적인 사항은
스마트폰 제조사의 공식 매뉴얼을 참고하세요.

네트워크 설정

애플과 마찬가지로 구글에서도 본격적으로 안드로이드 기기의 근처에 있는 다른 기기의 블루투스 정보를 사용하여 분실된 기기의 위치를 찾아주는 기술을 도입하였습니다.[40] 이는 내 기기나 내 주변에 있는 기기들에 대한 블루투스 정보가 구글에 의해 대규모로 수집될 수 있음을 뜻합니다. 이러한 정보가 수집되는 것을 거부하고 정보 수집에 쓰일 만한 기능을 비활성화하고자 한다면, 다음과 같은 절차를 따르세요.

와이파이, 블루투스 등은 사용하지 않을 때에는 꺼 두세요.
또한 '테더링 및 휴대용 핫스팟'도 사용하지 않을 때에는 꺼 두세요.
대체로 [설정] → [무선 및 네트워크] → [더 보기] → [테더링 및 휴대용 핫스팟]에서 비활성화할 수 있습니다.

위치 설정

안드로이드에는 구글에서 위치 정보를 지속적으로 수집하여 동선을 기록할 수 있도록 하는 Timeline이라는 기능이 내장되어 있습니다.[41] 이러한 기능을 활성화하면 나의 동선을 기록한다는 것을 빌미로 나의 위치 정보가 그대로 Google 등의 회사로 지속적으로 전달되어 위치 추적의 위험을 늘리게 됩니다. GPS와의 통신 때문에 배터리 소모 또한 늘어납니다. 따라서 위치 추적 등의 위협을 피해야만 하는 상황에서는 반드시 GPS를 끄도록 합니다.

대체로 [위치 서비스] → [무선 및 GPS 위치], 혹은 [설정] → [개인 설정] → [위치] → [모바일 데이터]에서 비활성화할 수 있습니다.

---

40 https://support.google.com/product-documentation/answer/14796936?sjid=13870903760616817433-AP
41 https://support.google.com/accounts/answer/14200149?authuser=0&hl=ko&visit_id=638571796252554111-689188657&p=timeline&rd=1

소프트웨어 업데이트

스마트폰의 운영체제와 스마트폰에 설치된 앱들은 지속적으로 공격 대상이 되며, 따라서 새로운 보안 취약점이 발견될 때 이에 대한 업데이트가 이뤄지기 마련입니다. 따라서 스마트폰 운영체제 자체의 업데이트, 설치된 앱의 업데이트가 있다면 안전성을 확인하고 설치하도록 합니다.

디지털 보안을 위한 안드로이드 앱

아래 목록은 2015 디지털 보안 가이드북의 안드로이드 앱 중 일부를 발췌한 것입니다.[42]

Orbot : 토르(Tor) 네트워크를 사용하여 스마트폰 내의 네트워크 활동의 익명성을 증가시키도록 설계된 앱입니다.[43]

Tor Browser for Android : 토르(Tor) 네트워크를 사용하는 웹 브라우저입니다. 스마트폰의 모든 네트워크 활동이 아닌 웹 브라우저 활동만을 토르 네트워크를 통하고자 할 때 유용합니다. Orweb → Orfox → Tor Browser 로 계승되었습니다.[44]

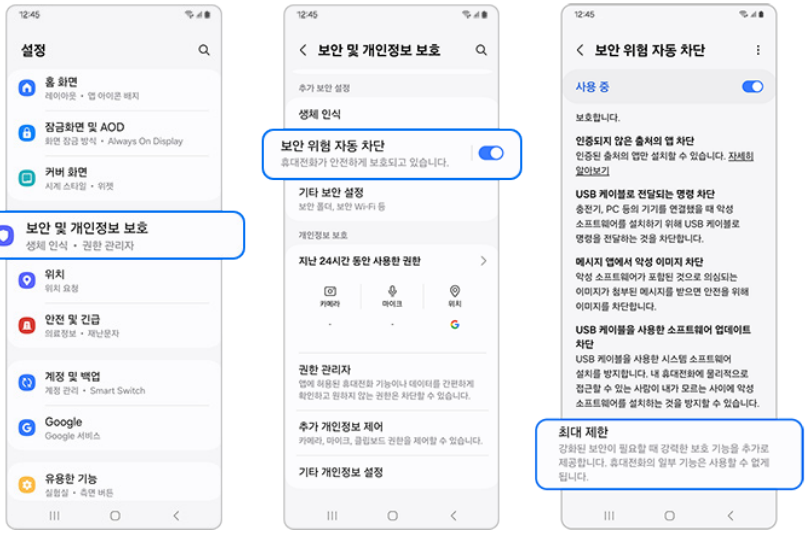
Firefox / Firefox Focus : 모바일용 파이어폭스 브라우저입니다.[45] [46]

'최대 제한' 설정

삼성 갤럭시 안드로이드 스마트폰을 사용하는 경우, 안드로이드

42 https://guide.jinbo.net/digital-security/smartphone-security/android-security-setting
43 https://securityinabox.org/en/guide/orbot/android
44 https://play.google.com/store/apps/details?id=org.torproject.torbrowser&hl=ko&pli=1
45 https://play.google.com/store/apps/details?id=org.mozilla.firefox
46 https://play.google.com/store/apps/details?id=org.mozilla.focus&hl=en

버전 14부터 '최대 제한' 기능을 사용할 수 있습니다.[47]
스미싱 공격 집중 등 복잡한 디지털 보안 공격을 받고 있는 상황에서는
'최대 제한' 설정을 통해 스마트폰의 보안성을 높여보세요.
[설정] → [보안 및 개인정보 보호] → [보안 위험 자동 차단] →
[최대 제한]의 순서로 찾아서 활성화할 수 있습니다.



4-3-3. 아이폰 보안 설정

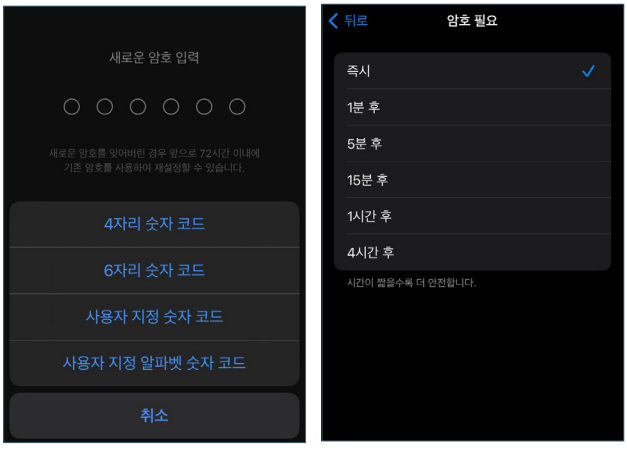
아이폰(iPhone)이나 아이패드(iPad)를 비롯해 애플(Apple)에서
만든 스마트폰, 스마트기기를 사용할 경우 필요한 보안 설정들을
살펴봅시다. 애플의 개인정보 보호 페이지[48]도 살펴보세요.

'암호'를 복잡한 비밀번호로 설정하기

47 https://www.samsungsvc.co.kr/solution/1711930
48 https://www.apple.com/kr/privacy/features/

아이폰에 저장되는 모든 정보는 아이폰에 설정하는 비밀번호, 즉 '암호'에 의해 암호화됩니다. 생체 인증 뿐만 아니라 '암호'를 꼭 설정해야 하는 이유입니다. 아주 오래된 구형 아이폰(iOS 8 이전)에서는 4자리 숫자, iOS 9 이후 버전에서는 6자리 숫자로 설정할 수 있지만, 좀더 높은 보안을 위해서는 <비밀번호와 인증>에서 살펴본 것처럼 조금 더 복잡한 형태로 설정하는 것을 권장합니다. 다만 아이폰의 '암호'는 아이폰을 껐다 켤 때 매번 입력해야 한다는 점을 잊지 마세요.

[설정] → [Face ID 및 암호], 혹은 [설정] → [Touch ID 및 암호], 혹은 [설정] → [암호] 메뉴로 가서 암호를 설정합니다. 이때 [옵션]으로 들어가서 [사용자 지정 숫자 코드]를 써서 더 긴 자릿수의 숫자로 설정하거나, 아니면 [사용자 지정 알파벳 숫자 코드]를 써서 숫자와 알파벳을 섞어서 설정하세요.

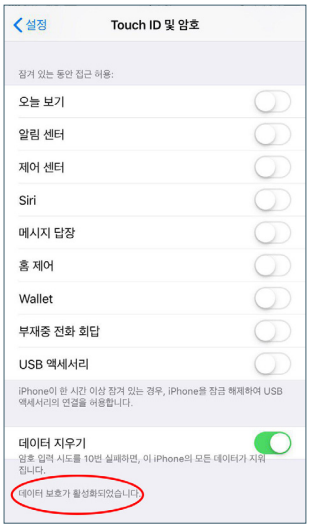


암호를 설정했으면 [암호 필요] 항목을 [즉시]로 설정하세요.

이제 암호 메뉴로 돌아가서 스크롤을 맨 밑까지 내리면, "데이터 보호가 활성화되었습니다"라는 메시지가 보입니다. 기기에 있는 대부분의

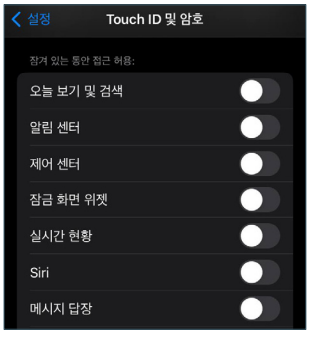
데이터에 접근하기 위해 암호가 필요하도록 암호화가 잘 이뤄졌습니다. 누군가 전원이 꺼진 당신의 아이폰을 입수하더라도 복잡한 비밀번호를 입력해내지 못하면 기기에 저장된 데이터를 꺼내기 어려워졌음을 뜻합니다. 다만, 방심은 금물입니다. 유능한 공격자라면 당신의 아이폰과 함께 당신의 비밀번호도 가져갈 수 있으니까요.

데이터 지우기 옵션 활성화



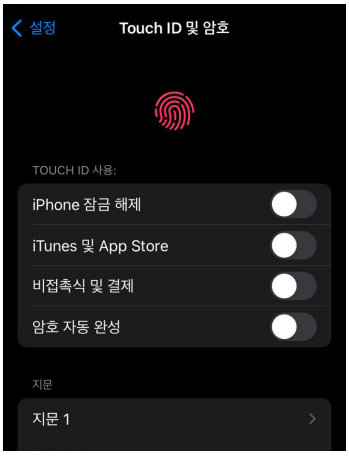
암호를 모르더라도 암호를 알아내기 위해 가능한 모든 경우의 수를 시도해 보는 집념 앞에서는 아이폰의 암호화 만으로는 충분하지 않을 수도 있습니다. 집회나 시위에 참석했다 혹시 아이폰을 잃어버릴 가능성이 있고, 데이터가 유출되는 것보다 차라리 삭제되는 것이 낫다면, 암호 메뉴에서 [데이터 지우기] 옵션을 활성화하세요. 암호를 10번 틀리면 아이폰에 저장된 모든 데이터를 삭제합니다.

잠금 화면에서 할 수 있는 작업 제한



아이폰의 잠금 화면에서 [알림 센터]를 통해 다양한 정보가 노출될 수 있습니다. 편리성을 위해 메신저에 온 메시지의 내용이 [알림 센터]에 표시되는 등 개별 앱마다 잠금 화면에 노출시킬 수 있는 정보가 생각보다 광범위할 수 있습니다. 잠금 화면에서 할 수 있는 작업은 꼭 필요한 것만 허용하세요.

생체 인증으로 할 수 있는 작업 제한



집회나 시위 현장에 참석할 때는 생체 인증을 사용하여도 아이폰 잠금을 해제할 수 없도록 설정하는 것이 안전할 수 있습니다. 평소에는 편리하게 아이폰 잠금을 해제하기 위해 지문 인식을 사용하더라도, 집회나 시위 현장에 참석할 때는 안전을 위해 비활성화하는 걸 고려하세요.

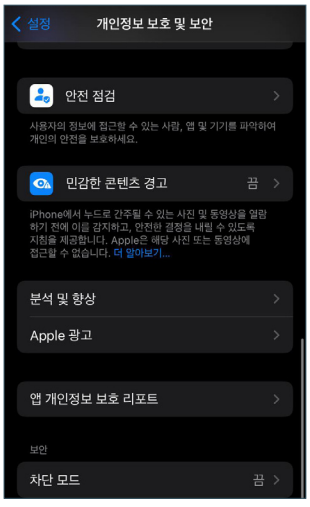
아이클라우드(iCloud) 보안 설정

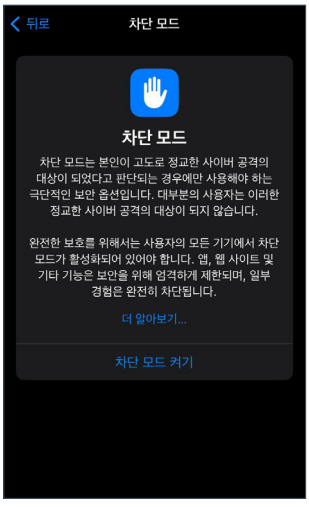
아이폰 내에는 데이터가 암호화되어 저장되어 있어도 아이폰과 아이클라우드를 연동하여 데이터가 자동으로 백업되고 있다면, 그리고 아이클라우드의 비밀번호가 매우 단순하다면, 공격자는 아이폰 대신 아이클라우드 쪽을 노려서 아이폰에 저장된 데이터를 확보할 수도 있습니다. 아이클라우드 계정의 비밀번호 또한 충분히 안전하게 유지하세요.

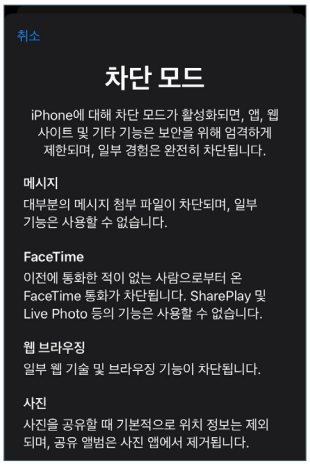
차단 모드(LockDown 모드) 설정

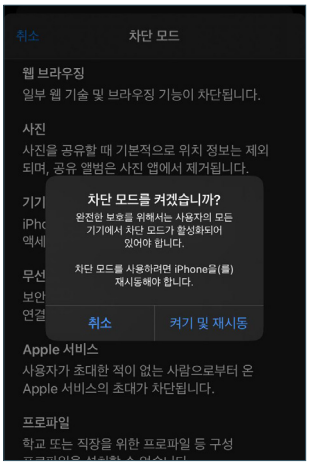
집회나 시위 현장에 참석할 때, iOS 16 이상의 버전을 사용중인 경우 차단 모드(LockDown) 설정을 고려할 수 있습니다.
차단 모드(LockDown)에서는 iMessage의 링크 미리보기 기능을 비롯해

잠재적인 보안 위험을 가져올 수 있는 기능들이 차단되며, 다른 사람에게 사진을 공유할 때 위치 정보를 자동으로 제거합니다. 차단 모드는 통상적인 악성코드에 기반한 보안 위험들에 대한 대응책입니다. 따라서 집회나 시위 현장에 참석할 때 다른 보안 대책과 함께 활성화하고, 집에 안전히 귀가한 뒤 비활성화하는 것을 고민해 보세요. 차단 모드 활성화는 [설정] → [개인정보 보호 및 보안] → [차단 모드]에서 설정할 수 있습니다.









차단 모드에 대한 더 자세한 정보는 다음의 자료들을 참고하세요.

- 애플 - 차단 모드에 관하여 https://support.apple.com/ko-kr/105120
- (영문) How to: Enable Lockdown Mode on iPhone (Surveillance Self-Defense) https://ssd.eff.org/module/how-to-enable-lockdown-mode-on-iphone

5. 통신, 이메일 및 메신저 보안

5-1. 통신 보안의 이해

5-1-1. 통신 보안에서 암호화가 중요한 이유

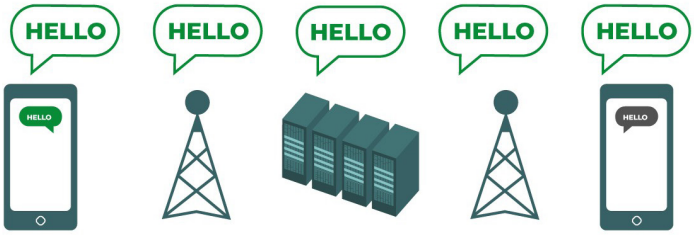
일반적으로 암호화(Encryption)란, 복호화(Decryption) 수단 없이는 내용을 알 수 없도록 정보를 변환하는 과정을 말합니다. 인터넷을 비롯한 다양한 통신 기술이 발전하면서 정보를 저장하고 전달하기가 매우 쉬워졌지만, 동시에 전달되는 정보가 감시의 대상이 되기도 쉬워졌습니다. 정보를 저장하고 전달할 때 암호화가 반드시 필요한 이유입니다.

암호화 없는 통신의 위험성

인터넷을 통해 전송되는 모든 정보는 다양한 형태로 감시당할 수 있습니다. 이메일 계정의 비밀번호를 매우 어렵고 복잡하게 설정해 두어도 정작 이메일 내용 자체가 암호화되지 않은 채 인터넷을 통해 전송되면 이메일 내용이 그대로 유출될 수 있습니다. 실제로 2020년 10월, 암호화 없는 통신을 사용하던 한 포털 서비스의 이메일 내용이 패킷 스니핑(Packet Sniffing)이라는 간단한 해킹 기법으로 유출될 수 있다는 사실이 기사화되기도 했습니다.[49] 해당 포털 사이트는 암호화되지 않는 통신 방식을 사용하는 모바일 웹 페이지를 유지하고 있었고, 이 모바일 웹 페이지를 써서 자신의 이메일 내용을 살펴볼 때 그 내용을 중간에서 가로챌 수 있었던 것입니다. 스마트폰으로 메시지를 주고받는 상황을 예로 들어보면 좀더 이해가 쉽습니다.[50]

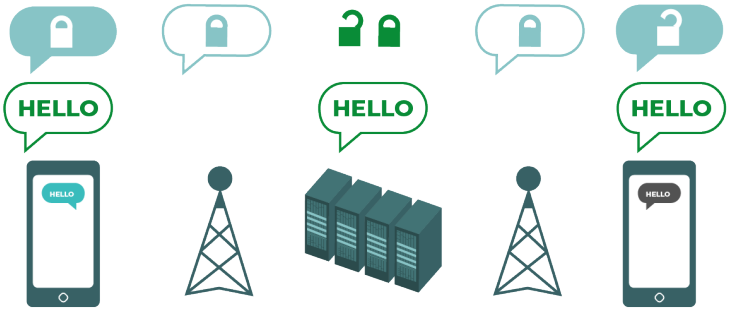
---

49 https://www.hankyung.com/article/202010132731i
50 https://ssd.eff.org/module/what-should-i-know-about-encryption#encrypting-data-in-transit



위 그림은 두 대의 스마트폰으로 서로 메시지를 주고받을 때 암호화가 전혀 없는 상황을 소개하고 있습니다.[51] HELLO라는 메시지는 내 스마트폰, 메시지를 받을 상대방의 스마트폰뿐만 아니라 통신사 기지국, 메신저 서비스 서버 등 여러 곳을 거쳐갑니다. 거쳐가는 곳에 있는 누구든 메시지의 내용을 읽을 수 있다는 말입니다.

전송 계층 보안(https, TLS)의 중요성

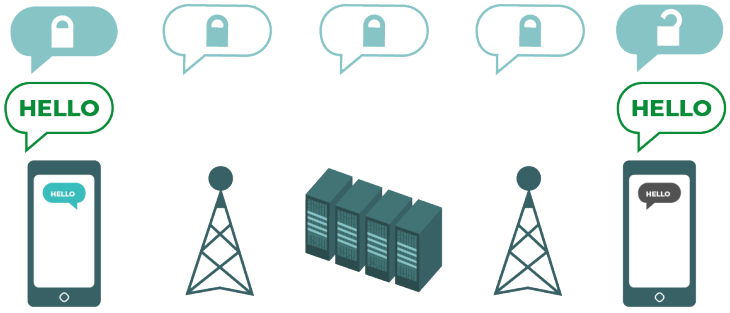


위 그림은 두 대의 스마트폰으로 서로 메시지를 주고받을 때, 전송 계층 암호화가 적용된 상황을 보여주고 있습니다. HELLO라는 메시지는 내

51 https://ssd.eff.org/module/what-should-i-know-about-encryption#transport-layer-encryption

스마트폰과 메신저 서비스 서버, 그리고 상대방의 스마트폰에서만 열어볼 수 있도록 암호화되어 전송됩니다. HELLO라는 메시지가 내 스마트폰에서 메신저 서버로 전송될 때 그 중간에서 거쳐가는 통신사 기지국에서는 암호화된 내용을 열어볼 수 없습니다. 마찬가지로 메신저 서버에서 상대방의 스마트폰으로 전송될 때 그 중간에서 거쳐가는 통신사 기지국 또한 암호화 내용을 열어볼 수 없습니다. 하지만 내 스마트폰, 메신저 서비스 서버, 그리고 상대방의 스마트폰에서는 메시지의 내용을 열어볼 수 있습니다.

종단간 암호화 (End-to-end Encryption, E2EE)



위 그림은 종단간 암호화가 적용된 상황에서의 통신을 다루고 있습니다.[52] 메시지를 보내는 스마트폰, 메시지를 받는 스마트폰에서는 메시지 내용을 볼 수 있지만, 메시지가 거쳐가는 동안에는 통신사 기지국이나 메신저 서버 등 메시지가 경유하는 그 어느 곳에서도 메시지의 내용을 볼 수 없도록 암호화가 적용되는 상황을 보여줍니다.

52 https://ssd.eff.org/module/what-should-i-know-about-encryption#end-to-end-encryption

5-1-2. 암호화와 공개키 암호화, 종단간 암호화

실질적으로 통신에 있어 암호화, 공개키 암호화, 종단간 암호화가 무엇인지에 대한 설명은 2015년도 디지털 보안 가이드의 <암호화란 무엇인가>[53], <공개키 암호화와 PGP에 대한 소개>[54], <종단간 암호화와 안전한 통신>[55]을 살펴보세요.

53 https://guide.jinbo.net/digital-security/communication-security/what-is-encryption
54 https://guide.jinbo.net/digital-security/communication-security/introduction-public-key-encryption
55 https://guide.jinbo.net/digital-security/communication-security/e2e-encryption

5-2. 메신저 보안

5-2-1. 메신저 선택 가이드

메신저를 선택함에 있어 디지털 보안을 최우선으로 생각한다면 다음의 네 가지 질문을 떠올릴 필요가 있습니다.

'모든 대화'에 기본적으로 종단간 암호화를 지원하는지?

메신저의 보안성을 자랑하는 메신저 서비스들 중 일부는 메신저 자체의 편의성을 위해 '모든 대화'가 아닌 '일부 대화'에만 종단간 암호화를 지원하기도 합니다. 텔레그램이 바로 그런 경우입니다.[56] 종단간 암호화가 메신저 사용에 있어 필수적이라는 판단을 하고 있다면, 시그널처럼 '모든 대화'에 기본적으로 종단간 암호화를 지원하는 메신저를 사용할 필요가 있습니다.

클라우드 등에 메신저 대화 데이터를 저장하는지?

텔레그램 등의 일부 메신저는 기본적으로 클라우드 등에 메신저로 주고받은 파일, 대화 데이터 등을 영구적으로 저장합니다. 이는 해당 메신저 사용의 편의성을 증대시켜주지만, 동시에 당신의 통제 범위 바깥에 당신의 대화 데이터를 보존한다는 것을 의미하기도 합니다.

정부 기관, 혹은 관리자의 요청에 따라 대화 데이터를 제공하는지, 혹은 제공할 수 있는지?

'모든 대화'에 기본적으로 종단간 암호화를 지원하는 메신저라면

56 https://telegra.ph/Why-Isnt-Telegram-End-to-End-Encrypted-by-Default-08-14

정부 기관이나 관리자가 요청하더라도 대화 데이터를 제공할 수 없을 것입니다. 하지만 그렇지 않은 메신저라면, 정부 기관이나 관리자의 요청에 의해 대화 데이터를 제공할 의향이 있는지, 그리고 그러한 상황에 대해 공개적으로 어떤 입장을 밝히고 있는지를 알아보는 것이 메신저 선택에 있어 판단기준이 될 수 있습니다.

더 나은 암호화 방식 지원을 위한 연구개발을 지속하고 있는지?

완전무결한 암호화 방식은 존재하지 않습니다. 과거에는 안전했던 암호화 방식도 미래에는 쉽게 보안 취약점이 발견되어 뚫릴 수 있습니다. 더 나은 암호화 방식을 지원하기 위해 지속적으로 연구개발을 하고 있는지는 해당 메신저를 계속 사용하여도 괜찮은지에 대한 지표가 됩니다.

예를 들어, 2024년 현재 많이 활용되고 있는 암호화 방식 중 상당수가 양자컴퓨터가 도입되면 수학적으로 암호화가 뚫릴 수 있습니다. 이로 인해 아주 낮은 가능성이지만 일어날 수 있는 보안 위협 시나리오가 있습니다. 바로 국가기관이나 통신사가 전 세계에서 일어난 통신을 모두 감청하여 수집하고 양자컴퓨터가 나올 때까지 보존하는 시나리오입니다. 종단간 암호화로 보호된 통신 내용 자체를 '지금은' 해독할 수 없겠지만, 수십 년 뒤에 양자컴퓨터가 상용화된 이후에는 쉽게 해독할 수 있다는 문제가 있습니다.

물론 양자컴퓨터의 상용화는 핵융합 등과 함께 매우 오랜 시간이 걸릴 일이지만, 먼 미래에라도 양자컴퓨터에 의해 보안이 해제되지 않을 방법이 있다면 좋겠습니다.

애플의 iMessage는 이에 2024년부터 자체적인 '양자내성암호'를 도입했습니다. '양자내성암호'는 설령 양자컴퓨터 개발이 완료되고

암호화된 통신내용이 모두 양자컴퓨터에 제공되더라도 수학적으로 뚫리기 어려운 암호를 말합니다. 보안 메신저 시그널(Signal)도 2023년에 '양자내성암호'[57]를 이미 도입했습니다.[58] 어떤 메신저를 고를지 고민할 때 '양자내성암호' 지원 여부는 좋은 기준이 됩니다.

5-2-2. 시그널(Signal) 설정 가이드

시그널(Signal)은 종단간 암호화를 채택하고 있는 오픈소스 메신저 소프트웨어입니다. 스마트폰(iOS, 안드로이드) 및 PC(윈도우, 맥, 리눅스)에서 사용할 수 있습니다. 시그널은 모든 대화에서 종단간 암호화를 채택하고 있어, 문자, 음성, 영상 대화 등을 암호화된 상태로 주고받을 수 있습니다.

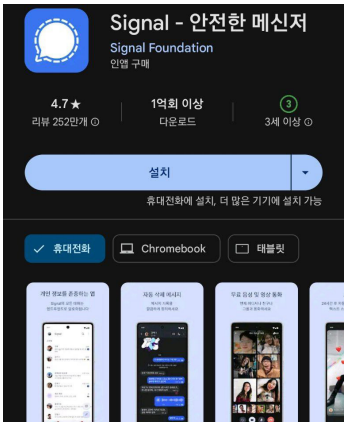
시그널의 제약 조건

시그널을 사용하려면 휴대전화번호가 있어야 합니다. 또한 PC에서 시그널을 사용하려면 먼저 스마트폰에서 시그널을 사용해야 합니다.

시그널 설치 및 가입하기

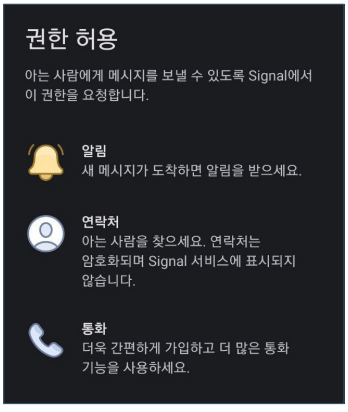
시그널 공식 한국어 웹 사이트(https://signal.org/ko/)의 [Signal 다운로드]의 안내에 따라 시그널을 설치하세요. 혹은 아이폰 앱스토어나 안드로이드 플레이스토어에서 시그널을 설치하세요.

57 https://security.apple.com/blog/imessage-pq3/
58 https://signal.org/blog/pqxdh/

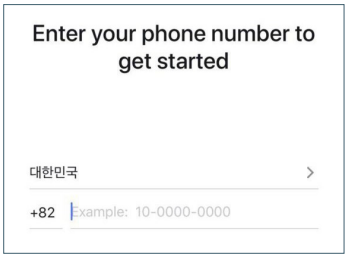


주소록 등 권한 부여하기

- 설치가 끝나면 시그널(Signal)에서 권한 부여를 요청합니다.
  어떤 권한이 부여되는지 확인하고 권한을 부여합니다.
  권한을 부여하지 않아도 시그널을 사용할 수는 있습니다.



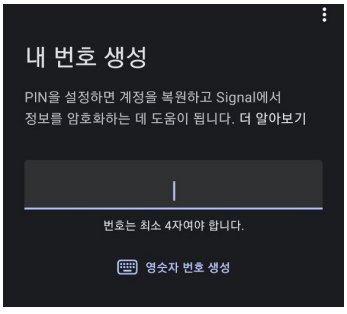
- 이제 전화번호 입력 화면으로 넘어갑니다.
  한국에서 010-XXXX-YYYY 번을 사용중이라면 10-XXXX-YYYY 를 입력합니다.
  (맨 앞의 0을 입력하면 시그널에서 전화번호를 인증할 수 없습니다.)



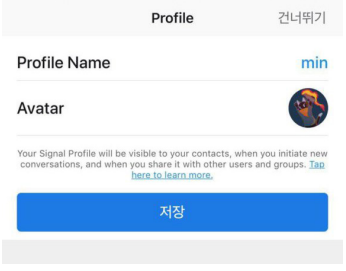
이제 문자메시지로 6자리 코드가 전송됩니다.

PIN 번호 설정하기

- PIN 번호는 시그널 계정을 보호하기 위한 수단입니다. PIN을 설정하지 않아도 시그널을 사용할 수 있지만, 휴대전화를 교체하거나 잃어버리면 시그널 계정을 새로 만들어야만 합니다. PIN을 만들기 전에, PIN을 잊지 않고 보존할 방법을 고민하세요. <비밀번호 관리 도구>에 넣어두는 것도 한 가지 방법입니다.
- PIN 번호까지 설정했으면, 이제 계정을 만들 준비가 다 끝났습니다.



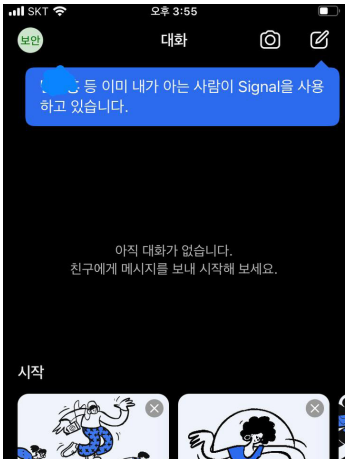
프로필 정보 입력하기

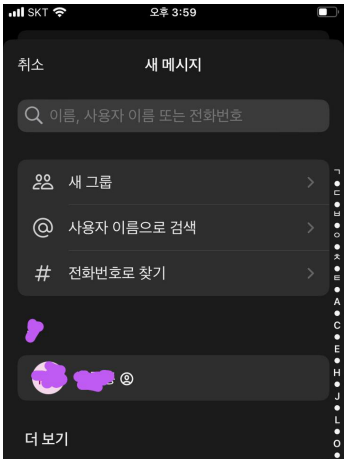


- 시그널을 사용중인 다른 사람들에게 표시될 프로필 정보를 입력합니다. 이때 내 휴대전화 번호가 있는 사람이 나를 찾을 수 있도록 할 것인지 결정할 수 있습니다. [모두에게 금지] 옵션을 선택하면 휴대전화 번호만으로는 상대방이 나에게 시그널 메시지를 보낼 수 없습니다.
- 이렇게 하여 시그널 가입을 마칩니다.

시그널 메시지 보내기

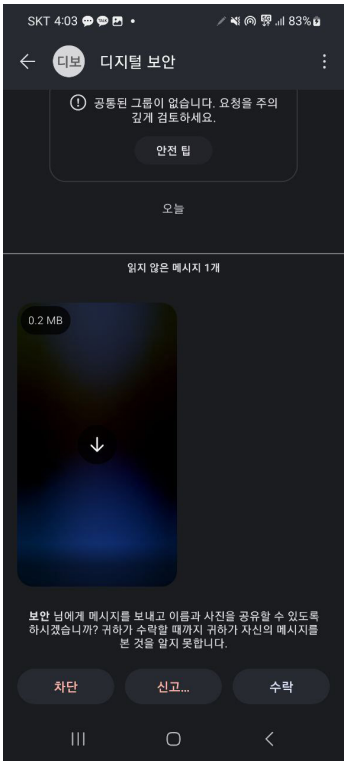
시그널 설치 시 주소록 권한을 부여했으면, 내 주소록에 전화번호가 저장되어 있으면서 시그널을 사용중인 사람들을 찾을 수 있습니다. 오른쪽 상단의 [새 메시지 보내기] 아이콘을 터치합니다. 주소록에 저장된 사람을 찾을 수 있습니다.





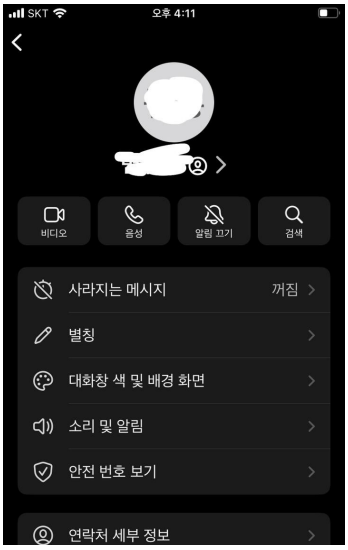
시그널 메시지 받기

나와 한 번도 시그널로 메시지를 주고받은 적이 없는 사람이 메시지를 보내면 아래와 같은 경고 메시지가 표시됩니다. [수락]을 누르면 상대가 보낸 메시지를 볼 수 있게 됩니다.

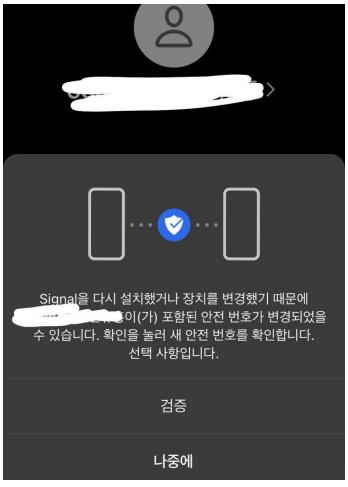


시그널 대화 상대 검증하기

상대방과 시그널 메신저를 사용하여 대화를 주고받기 시작하면 종단간 암호화를 위한 '안전 번호'가 생성됩니다. 상대방과 직접 만나는 자리에서 '안전 번호'를 서로 확인하면 좀더 안심하고 암호화된 대화를 나눌 수 있습니다. 대화창에서 상대방의 이름을 터치해 연락처 정보 화면으로 들어가면 아래와 같이 [안전 번호 검증] 메뉴를 선택할 수 있습니다.

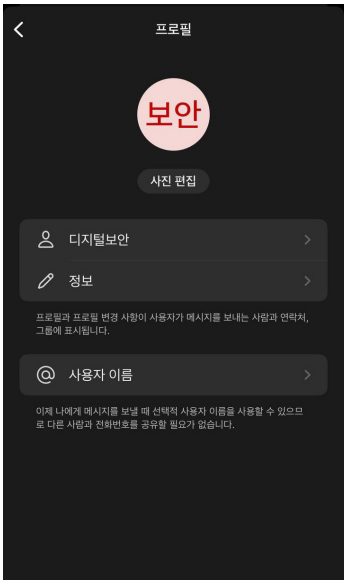


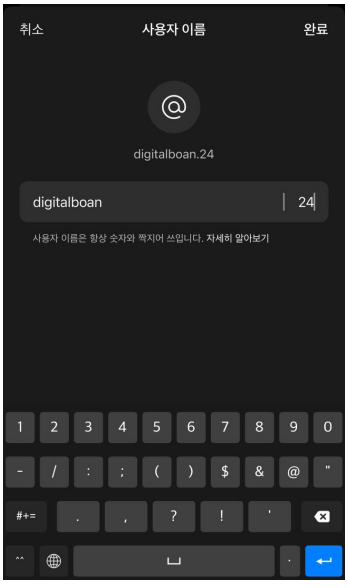
서로 만나 안전 번호를 확인했으면 [검증으로 표시]를 터치하면 됩니다. 만일 상대방이 휴대전화 기기를 변경했다면 '안전 번호'가 변경됩니다. 낮은 확률이지만 상대방의 휴대전화 번호를 빼앗고, PIN 번호 등을 모두 알고 있는 다른 존재가 상대방을 사칭할 가능성이 있기 때문에, 이러한 경우 다시 상대방을 직접 만나 '안전 번호'를 확인하면 다시 안심할 수 있게 됩니다.



시그널에서 전화번호 없이 메시지 주고받기

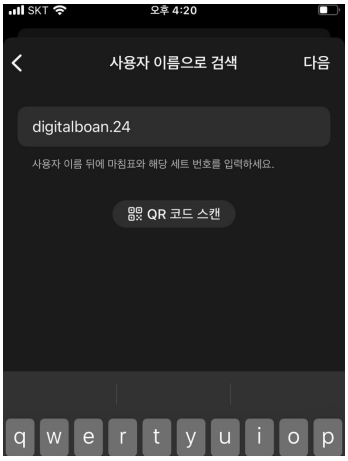
다른 사람에게 휴대전화번호를 알려주지 않으면서도 시그널 메신저를 사용하여 소통할 필요가 있을 때가 있습니다. 이런 경우를 위해 시그널은 [사용자 이름]을 설정할 수 있는 기능을 제공합니다. 사용자 이름은 알파벳 영문자와 숫자 2자리로만 만들 수 있습니다.
프로필 화면에서 아래 사진을 참고하여 사용자 이름을 등록하세요.

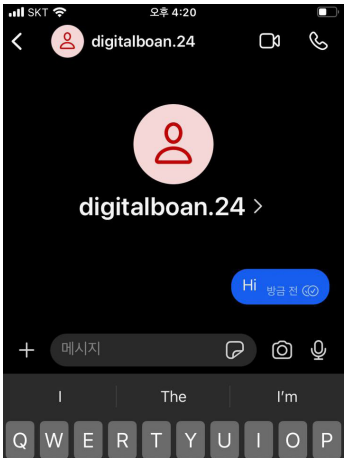


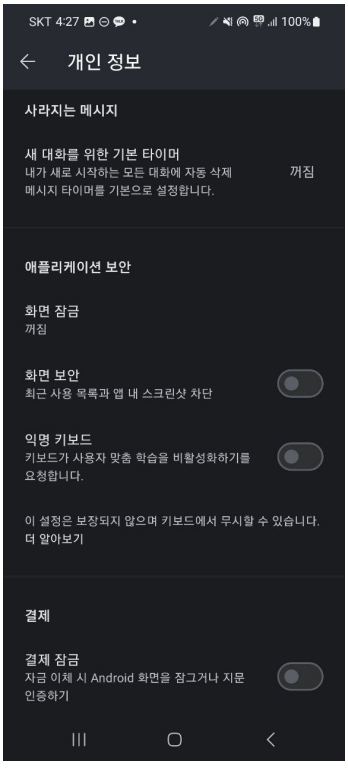


이제 나와 시그널로 메시지를 주고받아야 하지만 휴대전화번호를 알려주고 싶지 않은 다른 사람에게는 이렇게 만든 '사용자 이름'을 알려줍니다.

전달받은 '사용자 이름'으로 상대방을 찾기 위해
[새 메시지] 화면에서 [사용자 이름으로 검색]을 합니다.







시그널 추가 보안 설정

시그널은 다른 무엇보다 대화의 '보안'에 중점을 둔 메신저입니다. 상대방에게 보내는 메시지가 나와 상대방 모두의 휴대전화에서 일정 시간이 지나면 자동으로 사라지도록 하는 [사라지는 메시지] 설정, 시그널 앱 화면을 스크린샷으로 촬영할 수 없도록 하여 혹시라도 스크린샷이 클라우드에 올라가거나 하는 형태로 대화 내용이 유출될 가능성을 낮추기 위한 설정 등이 갖춰져 있습니다.

시그널 주의사항

시그널 메신저를 사용하더라도 어깨 너머로 휴대전화 화면을 볼 수 있는 사람에게 대화 내용이 노출되는 것은 막을 수 없습니다. 또한 내 휴대전화의 잠금을 해제할 수 있는 사람이 시그널 메신저의 대화 내용을 보는 것도 막을 수 없습니다.

스마트폰의 시그널 앱으로 주고받던 대화는 PC에 시그널 프로그램을 설치하고 계정을 연동하여도 그 이전까지 주고받던 대화를 PC에서 볼 수 없습니다. 특히 스마트폰을 바꿀 경우 (2024년 기준) 안드로이드 사용자가 아니면 대화 내용을 복원할 수 없는 점을 유의하세요.

5-2-3. 카카오톡 설정 가이드

지난 2014년, 세월호 집회를 주도했다는 이유로 전 노동당 부대표 정진우 씨의 카카오톡 메시지 내용이 압수수색되었습니다. 이는 카카오톡 서버에 대한 압수수색을 통해 이루어졌으며, 당사자조차 몇 개월 후에 이 사실을 알게 되었습니다. 정진우 씨 본인이 발신한 내용만 압수된 것이 아니었습니다. 단지 반일치 압수수색만으로 무려 2,368명의 대화 내용이 함께 압수된 것입니다. 이로 인해 한국의 많은 메신저 사용자들이 카카오톡에서 텔레그램 등의 타 메신저로 '망명'하게 되었습니다.

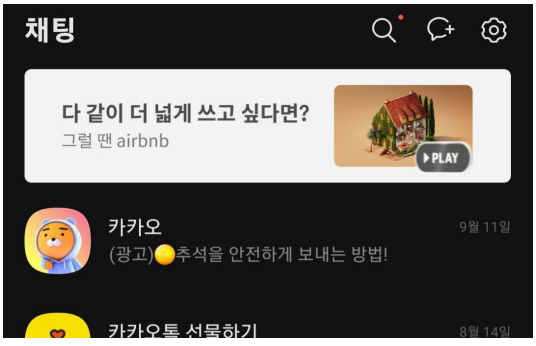
카카오톡은 이용자의 프라이버시를 보호하는 방향으로 서비스를 개편하였습니다. 평균 3~7일 서버에 저장하던 것을 2~3일만 대화내용을 저장하는 방식으로 변경하였습니다. 다른 보안 메신저들에서 지원되는 '종단간 암호화' 기술이 적용된 '비밀채팅'기능도 나왔습니다. 범죄 혐의점이 있는 경우 사실상 정보 소유자의 동의 없이도 카카오톡 서버를 압수수색할 수 있었던 수사기관의 관행에 대해서는 2022년 6월에서야 당사자의

참여권을 보장하지 않으면 위법하다는 대법원 판결도 나왔습니다.[59]

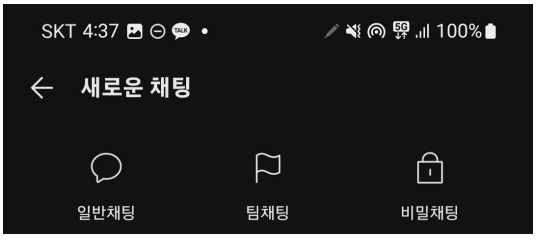
물론 여전히 카카오톡 서버가 한국 내에 있다는 사실은 외국의 메신저 서비스에 비해 한국 정부의 위협에 더 노출될 수 있는 요인이 될 수 있습니다. 이런 상황 속에서 카카오톡을 꼭 사용해야만 할 때 신경써야 하는 사안들을 살펴보겠습니다.

카카오톡 [비밀채팅] 기능 사용하기

카카오톡에서도 종단간 암호화 기반의 대화를 나눌 수 있습니다. 채팅목록 화면 우측 상단의 [새 대화] 아이콘을 터치해 주세요.

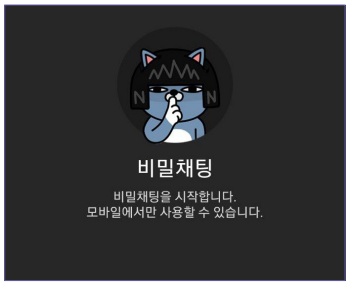


새로운 채팅 옵션 중 [비밀채팅]을 선택해 주세요.



59 https://news.kbs.co.kr/news/pc/view/view.do?ncd=5477371

종단간 암호화가 적용된 대화를 나눌 상대방을
선택하여 [비밀채팅] 창을 엽니다.



[비밀채팅]을 이용하여 나눈 대화는 PC버전
카카오톡에서는 사용할 수 없습니다.

카카오톡 사진 전송 시 메타데이터 유출 주의

카카오톡으로 사진을 주고받을 경우 고화질의 사진을 주고받기 위해
[원본] 화질을 선택하는 경우가 많습니다. 만일 사진 파일에 위치정보
등이 메타데이터로 저장되어 있을 경우 [원본] 화질로 선택하여 전송하면
사진 파일에 포함된 메타데이터 위치정보가 그대로 전달됩니다.

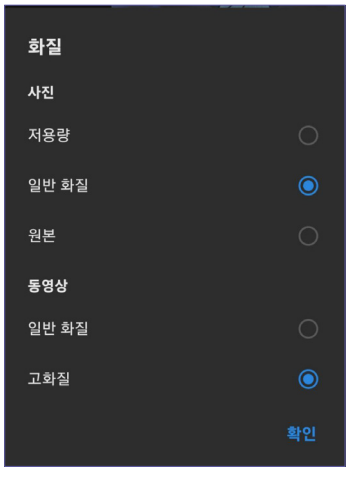


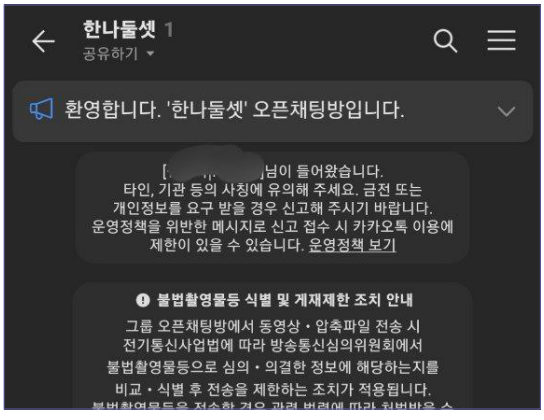
사진 파일에 메타데이터가 저장되어 있지 않도록 유지하는 것이
가장 좋지만 피치 못한 경우에는 [원본]이 아닌 화질 옵션을
선택하여 메타데이터가 전송되지 않도록 유의하세요.

카카오톡 [톡서랍 플러스] 기능 사용 시 유의

카카오톡은 모든 대화 내용 및 주고받은 사진 등 파일을 클라우드에
저장하고 언제든 열람할 수 있는 유료 서비스인 [톡서랍 플러스] 기능을
제공합니다. [톡서랍 플러스]를 사용하면 스마트폰을 변경해도
기존의 대화 이력을 온전히 보존할 수 있다는 장점이 있지만, 반대로
카카오톡 계정이 유출되면 [톡서랍 플러스]를 통해 다른 사람과
주고받은 파일이 빠르게 유출될 수 있다는 점에 주의하세요.

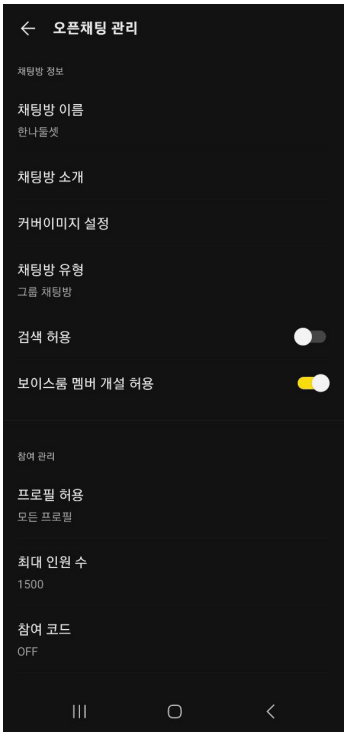
카카오톡 오픈채팅방에 참여코드 설정하기

카카오톡의 [오픈채팅] 기능을 사용할 경우, 오픈채팅방에 [참여코드]를
설정하는 것을 고려하세요. 불특정 다수와 소통하기 위한 목적으로
카카오톡 오픈채팅방을 사용하더라도, [참여코드]를 일부러 설정하여
불특정 다수의 오픈채팅방에 대한 공격행위를 한 단계 어렵게 만드세요.



오픈채팅방을 개설한 뒤, 화면 우측 상단의 메뉴를 터치합니다.

메뉴의 [오픈채팅 관리]로 들어갑니다.
[참여 코드]를 터치하고 참여 코드를 설정합니다.



5-2-4. 텔레그램 설정 가이드

텔레그램(Telegram)은 클라우드 기반 메신저로, 종단간 암호화로 보호되는 '비밀대화' 기능과 서버가 해외에 있어 한국 정부의 압수수색 영장 집행이 쉽지 않다는 점 등으로 각광받았습니다. 하지만 텔레그램의 모든 대화가 종단간 암호화로 보호되는 것은 아니며, '비밀대화'를 사용하지 않는 경우 주고받는 메시지 내용이 클라우드에 영구히 보존된다는 점에 유의해야 합니다. 계정 탈취 등의 보안 문제를 겪지 않기 위해

아래의 내용을 참고하여 텔레그램을 좀더 안전하게 사용하세요.

텔레그램 2단계 인증과 암호 잠금 활성화

텔레그램 메신저 설정의 [개인 정보 및 보안] 메뉴에서 [2단계 인증], [암호 잠금]을 활성화해야 합니다. [2단계 인증]을 활성화하고, 2단계 인증 사용 시 문제가 될 수 있는 지점을 명심해야 합니다.

텔레그램 미디어 자동 다운로드 기능 비활성화

2024년 7월 11일 공개되어 EvilVideo라고 명명된 텔레그램 보안 취약점은, 텔레그램 메신저 앱 상에서는 동영상 파일처럼 보이도록 위장한 악성 코드 설치 파일을 사용하는 공격입니다.[60]
최신 버전의 텔레그램 안드로이드 앱에서는 이 공격을 막을 수 있게 되었지만, 이런 방식의 해킹이 가능하다는 것을 알고 텔레그램 앱 자체가 이 공격을 막아주지 않더라도 스스로 막아낼 수 있어야 합니다.

이 보안 취약점은 아래와 같은 다섯 가지 단계를 모두 통과할 때

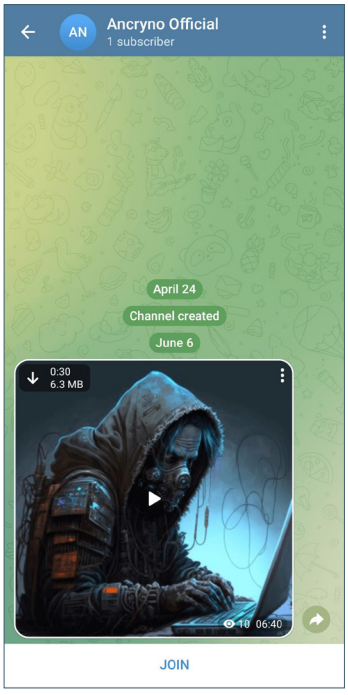
60 https://www.welivesecurity.com/en/eset-research/cursed-tapes-exploiting-evilvideo-vulnerability-telegram-android/

동작하며, 바꿔 말하면 이러한 단계 중 하나라도 어렵게 만들면 텔레그램 자체의 한계에도 조금이라도 더 안전을 보장할 수 있습니다.

텔레그램 메신저 내에서 동영상 파일을 자동으로 스마트폰으로 다운받지 않도록 설정하기

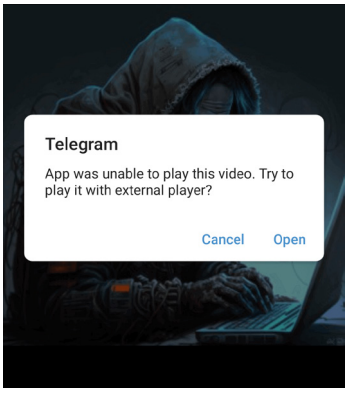
EvilVideo 텔레그램 보안 취약점은 동영상 파일로 위장한 악성 코드를 사용하며 실행되기 위해서는 동영상 파일로 위장한 악성 코드가 우선 스마트폰에 저장되어 있어야 합니다. 따라서 텔레그램 메신저의 [미디어 자동 다운로드] 설정을 변경하여 동영상 파일이 자동으로 스마트폰으로 다운받아지지 않도록 설정하면 한 차례 보안을 지킬 수 있습니다.

EvilVideo 공격에 사용되는 악성 코드는 텔레그램에서 아래 사진과 같이 동영상 파일로 인식됩니다. 믿을 수 있는 사람으로부터 전송된 동영상 파일이 아니라면 스마트폰에 저장 자체가 되지 않도록 하는 것이 한 단계 보안 강도를 높일 수 있습니다.



텔레그램 메신저 내에서 동영상을 재생하지 않기

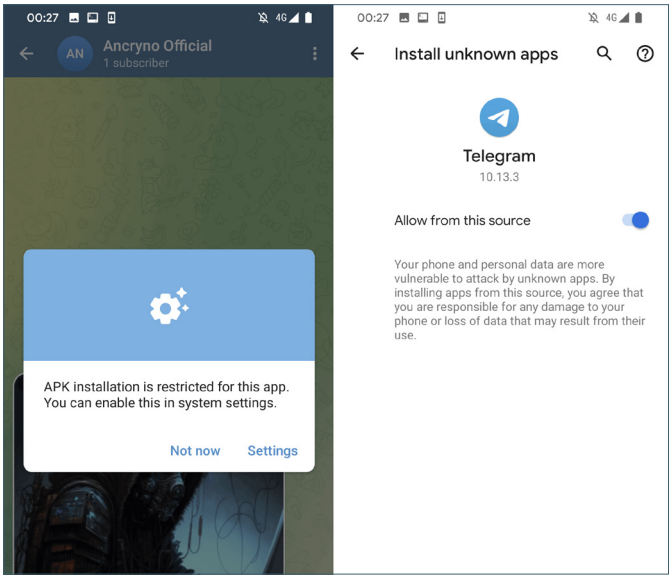
텔레그램 메신저 내에서 위의 동영상 파일을 재생하려고 시도하면 텔레그램 메신저는 아래 사진과 같이 [동영상 재생에 실패했으니 스마트폰에 설치되어 있는 다른(외부) 동영상 재생 앱을 써서 동영상을 재생하겠는지]를 사용자에게 물어봅니다. 이 단계에서 굳이 동영상을 재생하려는 시도를 하지 않는다면 EvilVideo 공격을 중간에라도 막을 수 있습니다.



텔레그램을 통해 앱이 직접 설치되지 않도록 설정하기

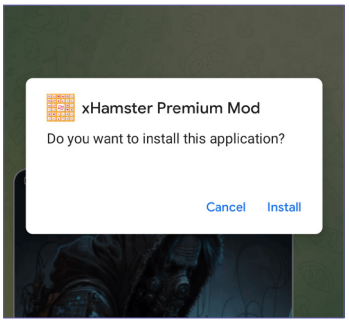
위의 단계에서 [열기](Open)를 선택하면, 이 파일은 악성 코드(앱) 설치 프로그램이기 때문에 안드로이드의 일반적인 보안 설정에 따라 APK 파일 기반의 설치를 허용할 것인지를 묻는 화면으로 넘어갑니다.

아래 사진처럼 이 단계에서 Setting(설정) 메뉴로 넘어가서 [출처를 알 수 없는 앱 설치 - 이 출처로부터 허용]을 설정하지 않는다면 악성 코드가 설치되는 상황을 막을 수 있습니다.



설치되는 앱의 이름을 보고 정말 지금 앱을 설치하는 게 맞는지 확인하기

주의를 충분히 기울이지 않아서, 텔레그램 메신저로부터의 앱 설치 자체를 한 차례 허용하게 되었다면, 지금 상황이 동영상 파일을 재생하려고 하는 상황이었을 뿐인데 앱 설치가 이뤄진다는 것이 무엇을 의미하는지 마지막으로 한 번 더 고민해 볼 수 있어야 합니다. 이 단계에서 마지막으로 주의를 기울여 앱을 설치하지 않기로 정한다면 EvilVideo 취약점을 통한 공격을 방어할 수 있습니다.



텔레그램 메신저 앱을 항상 최신 버전으로 유지하기

텔레그램 메신저 앱의 이러한 보안 취약점은 최신 버전의 텔레그램 메신저 앱에서는 더 이상 작동하지 않게 해결되었습니다. 즉 동영상으로 위장한 악성 코드 파일을 더 이상 동영상으로 인식하지 않게 된 것입니다. 하지만 이렇게 텔레그램 측에서 보안 취약점을 개선하더라도 사용자가 오래된 텔레그램 메신저 앱을 사용할 때에는 방법이 없습니다. 텔레그램 메신저 앱을 항상 최신 버전으로 유지해야 합니다.

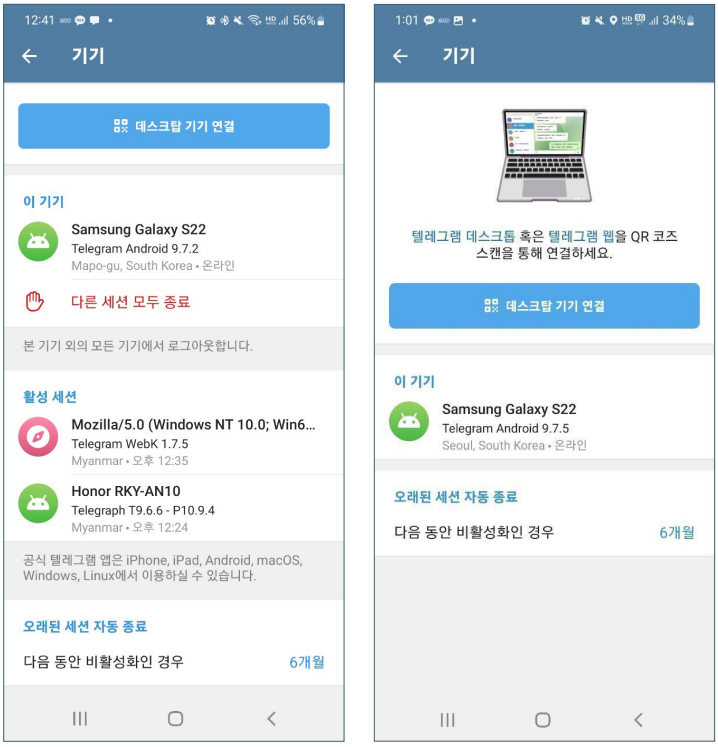
텔레그램 계정 탈취 시 다른 활성 세션 강제 종료하기

텔레그램 메신저의 계정이 탈취되었단 사실을 알게 되면 가장 먼저 해야 할 일은 공격자의 '활성 세션'을 강제로 종료하는 것입니다. 반대로 말하면, 텔레그램 메신저의 계정을 탈취한 공격자는 계정 주인의 '활성 세션'을 강제로 종료시키기 위해 노력할 것입니다.

텔레그램은 보안상의 이유로 인해 로그인 한 지 얼마 되지 않은 새로운 '활성 세션'이 기존의 '활성 세션'을 강제로 종료하지 못하도록 하고 있습니다. 반대로 말하면, 계정이 탈취되더라도 공격자가 그 즉시 계정 주인의 '활성 세션'을 종료시키지는 못한다는 말입니다.

[설정] → [개인정보 및 보안] → [기기들] → [활성 세션] 화면에서 활성 세션을 확인합시다. 아래 사진에서는 미얀마의 한 공격자에게 계정을 탈취당한 안드로이드 사용자의 화면이 보입니다.[61] 여기서 [다른 세션 모두 종료] 등을 선택하여 공격자가 더 이상 계정에 접근하지 못하도록 로그아웃시키도록 합니다.

61 https://www.edaily.co.kr/News/Read?newsId=01646566635679768&mediaCodeNo=257



5-2-5. 그 밖의 메신저 보안에 관하여

전반적인 메신저 보안에 대한 추가적인 읽을거리를 몇 가지 소개합니다.

- Front Line Defenders - <Guide to Secure Group Chat and Conferencing Tools>
  https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools
- 2015 디지털 보안 가이드 - <보안 메신저 – OTR+Pidgin>

https://guide.jinbo.net/digital-security/communication-security/how-to-use-otr-pidgin

5-3. 웹 브라우저 및 인터넷 보안

5-3-1. 인터넷 검열의 실태와 우회법

현대 한국의 인터넷 검열 실태에 대한 자세한 사항은 2015년 디지털 보안 가이드의 <온라인 검열을 우회하는 방법>을 참고하세요.[62] 윈도우에서 토르(Tor)를 사용하는 방법은 2015년 디지털 보안 가이드의 <윈도에서 토르(Tor) 사용하기>를 참고하세요.[63]

5-3-2. 가상 사설 네트워크(Virtual Private Network, VPN)

가상 사설 네트워크의 본래 목적은 인터넷을 통해 사무실 등의 내부에 있는 기기에 연결할 수 있도록 하는 것입니다. 조직의 사무실 내부에는 조직의 외부에 유출되면 곤란한 정보들이 많을 것이므로, 필요에 의해 잠시 인터넷을 거쳐 사무실 내부의 컴퓨터에 저장된 정보를 열람해야 하는 경우 데이터 전체를 추가적인 방법으로 암호화해야 합니다.

이러한 VPN의 특성은 정부나 통신사 등에 의한 온라인 검열을 우회하는 데 사용될 수 있습니다.[64] 예를 들어 특정 국가에서 들어오는 접속을 차단하는 서버가 있을 때, 해당 국가 내부에 마련된 VPN 서버를 경유하면 이러한 차단을 우회할 수 있습니다. 또한 특정 국가 내에서 정부 정책 등의 이유로 통신사에서 특정 서버를

62 https://guide.jinbo.net/digital-security/communication-security/circumvent-online-censorship
63 http://guide.jinbo.net/digital-security/communication-security/how-to-use-tor
64 https://guide.jinbo.net/digital-security/communication-security/circumvent-online-censorship

차단하고 있을 때, 외국에 있는 VPN 서버를 사용하면 해당 VPN 서버 자체가 차단되지 않는 한은 이러한 차단도 우회할 수 있습니다.

VPN은 태생적으로 회사나 기관 등의 조직에서 업무를 목적으로 운영하거나, 아니면 상업적 목적 혹은 비영리 목적으로 운영될 수 있으며, 최근에는 인터넷 공유기의 기능 중에 해당 인터넷 공유기 자체를 VPN 서버로 만드는 기능도 있어 지인들간의 별도의 암호화된 네트워크를 구성할 때 쓰이기도 합니다. 이러한 VPN 서버를 운영하는 'VPN 제공자'들은 VPN 서버를 경유하는 네트워크 활동이 정부나 통신사 등 제3자에 의해 가로채이지 않도록 보호합니다. 하지만 동시에 VPN 제공자들은 VPN 서버를 통해 누가 언제 어떤 웹사이트나 서버에 접속했는지를 기록할 수 있고, 이렇게 기록한 정보를 협박의 용도로 사용하거나 제3자에게 제공하는 일도 벌어질 수 있습니다. 따라서 VPN을 사용한다고 해서 반드시 인터넷 검열 우회와 디지털 보안에 도움이 되지는 않을 수도 있습니다. 믿을 만한 VPN인지의 여부를 판단할 수 있는 자신만의 기준을 마련하고, 이 기준에 따라 신뢰할 수 있는 것이 보장되는 VPN을 사용하세요.[65]

65 https://torrentfreak.com/best-vpn-anonymous-no-logging/

6. SNS, 홈페이지 보안

6-1. SNS 보안

6-1-1. SNS 보안의 기본

페이스북, 엑스(구 트위터), 인스타그램을 비롯한 SNS(Social Network Service), 소셜미디어(Social Media) 등은 인터넷으로 접근할 수 있는 가장 대중적인 공간입니다. 대부분의 SNS는 글, 사진, 혹은 사적인 정보를 다른 사람과 쉽게 공유할 수 있도록 만들어졌습니다. 때로는 어떤 주제에 대한 공론장의 역할을 수행하기도 합니다. 하지만 이 과정에서 SNS 사용 자체가 디지털 보안의 가장 취약한 지점으로 작용할 수 있습니다. 예를 들어, 당신의 비밀번호를 알아내려는 공격자가 당신의 SNS 계정에 공개된 정보를 토대로 당신의 주변 지인들의 신상정보를 알아내고, 하필 당신이 설정한 비밀번호가 당신의 가족의 생년월일이라는 점을 악용할 수 있습니다. 혹은 공격자는 당신의 SNS 계정을 사용하여 당신을 사칭하면서 거짓 정보를 유포하고자 할 수도 있습니다.

SNS를 사용하려는 목적을 달성하면서도 SNS가 디지털 보안의 가장 약한 연결고리가 되지 않게 하려면 어떻게 해야 할까요? 예를 들어, SNS를 사용하면서 동시에 익명성을 유지하려면 어떻게 해야 할까요? SNS를 통해 어떤 정보들을 공개하고, 어떤 정보들을 공개하지 않아야 할까요? 나 자신의 연락처가 SNS를 통해 노출되는 것은 괜찮은가요? 나 자신이 어떤 사람들과 관계를 맺고 있는지를 알 수 있는 사람의 범위를 어떻게 설정하고자 하나요? 결국, 핵심은 SNS를 통해 나 자신이 어떤 정보를 드러내고 싶고, 어떤 정보를 드러내지 않기를 원하는지, 어떤 정보가 노출되기를 원하고 어떤 정보가 노출되지 않기를 원하는지 명확히 알아야 한다는 것입니다.

SNS 계정을 생성할 때 점검할 사항들

실명 혹은 지인들이 아는 별명의 사용 여부

- 페이스북 등의 일부 SNS는 계정을 생성할 때 반드시 '실명'을 사용할 것을 요구합니다. 때때로 '실명'을 사용하지 않는 계정을 강제로 폐쇄하기도 합니다. 이는 해당 SNS 계정으로 진행하는 모든 활동이 나의 '실명', 즉 나 자신의 '신원'과 밀접하게 연관된다는 것을 뜻합니다. '실명'을 사용하지 않고 일부 지인들이 알고 있는 '별명'을 사용하여 SNS 활동을 하고 싶을 수도 있습니다. 이런 경우에도 해당 SNS 계정으로 진행하는 활동은 최소한 그 지인들에게는 나 자신의 활동이라는 것이 알려질 수 있다는 것을 뜻합니다. 완전한 익명성과 함께 SNS 활동을 하고 싶다면 '실명' 혹은 지인들이 알고 있는 '별명'의 사용에 유의하세요.

전화번호 혹은 이메일 주소, IP 주소 노출에 유의

- 대다수의 SNS는 주소록에 저장된 휴대전화번호 혹은 이메일 주소를 통해 해당 SNS를 이미 사용중인 지인을 쉽게 찾을 수 있도록 하는 기능을 제공합니다. 이런 방식으로 자신의 SNS 계정이 지인들에게 노출될 수도 있습니다. 익명성을 중요시한다면 SNS 계정 생성 과정에서 휴대전화번호나 이메일 주소를 비롯한 개인정보를 사용하지 마세요. SNS 계정만을 위한 별도의 이메일 주소를 사용하는 것이 한 가지 방법입니다. 또한 회원 가입 과정에서 IP주소 등의 형태로 자신에 대한 정보가 SNS 서비스 제공자에게 노출될 수 있음에 유의하세요.

프로필 사진을 통한 정보 노출에 유의

- SNS 계정의 프로필 사진을 통해 다양한 정보가 노출될 수 있습니다. SNS 계정을 만들면서 이름이나 이메일 주소 등을 전부 자신과 연관되지 않도록 하여도 정작 프로필 사진을 통해 자신의 신원을 노출하는 상황이 일어나서는 곤란합니다. 프로필 사진에 저장된 메타데이터의 위치정보, 혹은 사진에 촬영된 특정한 장소나 배경, 인물 등이 당신이 노출되지 않았으면 하는 정보를 담고 있지는 않은지 점검하세요.

강력한 비밀번호와 2단계 인증, 비밀번호 복구 질문에 유의

- 2단계 인증 등 보안성이 높은 인증 방식을 사용하는 것은 선택이 아닌 필수입니다. 최소한 비밀번호를 가능한 한 안전하게 설정해야 합니다. 때때로 이른바 '비밀번호 복구 질문'이라고 하여, 비밀번호를 잊은 경우에 대비해 "당신이 태어난 도시는 어디입니까?" 혹은 "당신의 반려동물의 이름은 무엇입니까?" 같은 질문 중 하나를 골라 이에 대한 답변을 입력해두도록 하는 웹사이트가 있습니다. 만일 이런 정보들을 자신의 SNS 계정을 통해 드러낸다면, 공격자는 당신의 SNS 계정을 통해 '비밀번호 복구 질문'에 대한 답을 알아내고 당신의 계정을 탈취하는 데 활용할 것입니다. 만일 계정을 생성할 때 이런 '비밀번호 복구 질문'에 대한 답을 반드시 입력해야 한다면, '비밀번호 복구 질문' 에 대한 답 또한 실제와는 다른 엉뚱한 것으로 설정하고 이를 마치 비밀번호처럼 관리하는 것이 나을 수도 있습니다. 직접 기억하기보다 [비밀번호 관리 도구]가 기억하게 하는 것도 방법입니다.

이용약관 및 개인정보처리방침 점검하기

새로운 계정을 만들 때 이용약관(Terms of Service)이나 개인정보처리방침(개인정보 보호 정책, Privacy Policy)을 꼼꼼히 읽어보는 것은 불가능에 가깝습니다. 하지만 최소한 다음의 내용들은 그래도 시간을 내어 꼼꼼히 살펴볼 필요가 있습니다. 어떤 데이터를 수집하는지, 수집한 데이터를 어떤 목적으로 어떻게 사용하는지, 제3자와 어떤 데이터를 공유하는지, 계정 삭제 시 내 데이터가 어떻게 삭제되는지, 영장 등의 사법기관 요청에 어떤 식으로 대응하는지에 대한 정보는 자신의 디지털 보안 대책과 직결되는 문제이므로, 이에 대한 내용은 따로 살펴볼 것을 권장합니다.

추적기 차단 브라우저 확장 도구 사용 검토

정교한 마케팅 목적 등의 이유로 상당수 SNS는 사용자가 직접 제공하지 않은 민감한 정보를 수집하는 경우가 많습니다. 예를 들어, 사용자의 위치,

관심사, 반응한 광고, SNS를 통해 방문한 다른 사이트에 대한 정보 등은 맞춤형 광고를 위해 광범위하게 활용됩니다. 사용자가 직접 제공하지 않은 민감한 정보를 수집하는 도구를 추적기(Tracker)라고 부릅니다. 만일 이러한 정보들이 나도 모르는 사이에 수집되는 것을 원하지 않는다면, 웹 브라우저를 사용하는 동안에는 제3자 쿠키 차단 및 추적기 차단(tracker blocking) 브라우저 확장 프로그램을 사용하여 불필요한 정보가 수집되지 않도록 할 수 있습니다. EFF에서 제공하는 추적기 차단 브라우저 확장 프로그램인 'Privacy Badger'를 사용하는 것도 한 가지 방법입니다.[66]

프라이버시 관련 기본값 설정 검토

SNS에 정보를 올릴 때 기본값으로 어떤 공개 설정이 적용되는지를 확인하고 검토하세요. 예를 들어, 게시물을 누구나 볼 수 있도록 모든 사람에게 공개할지, 아니면 당신의 SNS 계정과 이미 친구관계로 설정된 사람 혹은 그 사람들 중 일부만 볼 수 있도록 할지와 같은 설정의 기본값이 어떻게 되어 있는지를 검토해야 합니다. 혹은 당신이 계정을 만들 때 설정한 이메일 주소나 전화번호를 통해 다른 사람들이 당신을 찾을 수 있도록 허용할지의 여부를 확인해야 합니다. SNS에 정보를 올릴 때 위치 정보 또한 자동으로 공유되도록 설정되어 있을 수도 있습니다. 이러한 설정들 하나 하나가 당신의 디지털 보안 정책과 들어맞는지 확인하세요. 페이스북의 개인정보 상태 확인,[67] 구글의 개인정보 보호 진단[68] 등 프라이버시 관련 설정을 점검할 수 있는 기능이 제공되는 경우 이를 확인하세요.

프라이버시 관련 설정은 시간이 지남에 따라 변경될 수 있습니다. 설정이 강화되거나 세부적으로 변경될 수도 있지만, 반대로 완화될 수도 있습니다.

66 https://privacybadger.org/
67 https://www.facebook.com/help/443357099140264
68 https://myaccount.google.com/privacycheckup

프라이버시 관련 설정 변경 사항을 주의 깊게 살펴보고,
혹시 비공개였던 정보가 공개되도록 설정이 변경되지는 않는지,
이로 인해 개인정보 침해가 새롭게 일어나지는 않는지를 모니터링하세요.

'우리 편'에 의한 개인정보 침해 가능성

자기 자신의 SNS 계정과 관련된 개인정보 설정을 꼼꼼히 살피더라도,
SNS의 특성상 다른 사람에 의해 당신의 개인정보가 의도치 않게
노출될 수 있다는 점에 유의해야 합니다. 예를 들어 당신의 친구가 SNS에
당신의 사진을 올리면서 당신의 이름을 적어 넣는다거나, 혹은 당신의 계정을
태그하거나, 그 사진의 위치 정보를 공개한다면 친구의 SNS 계정이야말로
당신에 대한 개인정보를 얻을 수 있는 가장 약한 연결고리가 되는 셈입니다.
때로는 당신의 친구의 SNS 계정과 당신의 SNS 계정이 서로 연결되어
있다는 사실 그 자체가 공격자에게 많은 정보를 제공해 줄 수도 있습니다.
즉, 당신의 SNS 계정의 친구 목록, 혹은 당신의 친구의 SNS 계정의
친구 목록이 당신에 대한 공격의 수단이 될 수 있습니다.
SNS에서의 디지털 보안은 나 한 사람만의 문제가 아닌,
'우리 편' 모두에 대한 문제임을 명심하세요.

6-1-2. 주요 SNS별 디지털 보안 설정법

다양한 소셜 미디어 플랫폼이 있고, 각 플랫폼마다 적절한 디지털
보안 설정이 다릅니다. 페이스북에 대한 보안 설정은 2015 디지털
보안 가이드의 <페이스북 보안 설정>[69]을 참고하세요. 엑스(구
트위터)에 대한 보안 설정은 Security-in-a-box의 <트위터 보안

69 https://guide.jinbo.net/digital-security/communication-security/facebook-security-setting

설정>(영문)[70]을 참고하세요. 인스타그램에 대한 보안 설정은 Security-in-a-box의 <인스타그램 보안 설정>(영문)[71]을 참고하세요.

70 https://securityinabox.org/en/tools/twitter/
71 https://securityinabox.org/en/tools/instagram/

6-2. 홈페이지, 웹사이트 보안

6-2-1. '구글 해킹' 점검

2000년대 초반, 한국의 많은 관공서의 홈페이지, 웹사이트에 다른 사람에게 노출되어서는 안 될 '개인 정보'가 노출되어 있음이 구글 검색엔진을 통해 알려지는, 이른바 '구글 해킹'이라는 사태가 대대적으로 알려진 바 있습니다.[72] [73] 웹사이트나 홈페이지의 개발자는 로그인 등 특수한 절차를 거쳐야만 해당 파일들에 접근하는 것을 의도했지만, 구글 등의 검색엔진이 이런 절차를 생략하고 '개인정보' 파일에 접근할 수 있는 경우가 발견된 것입니다. 이로 인해 한동안 관공서 홈페이지나 웹사이트는 검색엔진에 어떠한 정보도 노출하지 말라는 취지의 권고가 내려진 것처럼, 구글 등의 검색엔진에 어떠한 정보도 수집되지 않도록 차단되는 일도 벌어지곤 했습니다.[74] 나아가 검색엔진에 노출되어서는 안 되는 정보가 웹사이트의 어느 경로에 있는지를 노출하는 방향의 권고가 내려지는 일도 있었습니다.[75]

홈페이지나 웹사이트를 운영중이라면, 이렇게 검색엔진을 통해 혹시라도 노출되어서는 안 되는 정보가 노출되고 있지는 않은지 점검할 필요가 있습니다. 운영중인 홈페이지나 웹사이트의 주소에 딸려 있는 정보가 검색되는지의 여부를 검색엔진에 입력하는 것입니다. 예를 들어 운영중인 사이트가 guide.jinbo.net 이라면, 구글 검색엔진에 site:guide.jinbo.net 이라고 입력하여 검색 가능한 정보가 어떤 것이 있는지 살펴볼 수 있습니다.

72 https://ko.wikipedia.org/wiki/%EA%B5%AC%EA%B8%80_%ED%95%B4%ED%82%B9
73 https://m.boannews.com/html/detail.html?idx=9853
74 https://slownews.kr/10883
75 https://www.hani.co.kr/arti/economy/it/607817.html

물론 검색엔진에 노출이 되지 않았다고 하여 홈페이지나 웹사이트 어딘가에 게시되어 있지만 모든 사람에게 공개되어서는 안 되는 정보가 안전하게 보호되고 있다고 생각해서는 곤란합니다. 웹사이트나 홈페이지 자체의 보안 수준을 점검하고, CMS 도구 등을 통해 웹사이트나 홈페이지를 구축한 경우 CMS의 보안 업데이트를 지속적으로 반영할 수 있도록 해야 하겠습니다.

6-2-2. 악성코드 유포 방지 및 백업

자체 구축 홈페이지나 웹사이트를 운영중인 경우, 홈페이지나 웹사이트를 통해 악성 코드가 유포되지 않도록 각별한 주의가 필요합니다. 관리자 권한이 있는 계정을 탈취하여 웹사이트 화면 혹은 공지사항 게시물에 악성 코드를 숨기는 경우가 대거 발견되고 있습니다.[76] 운영중이던 홈페이지나 웹사이트가 악성코드 유포 등의 진원지가 되어서도, 공격자의 공격이 성공한 채로 방치되어서도 곤란합니다.

게시물을 올릴 수 있는 권한이 있는 계정의 로그인 기록, 게시물 작성 및 수정 기록 등을 확인할 수 있는지, 모니터링할 수 있는 체계가 갖춰져 있는지 확인하고, 체계가 없다면 갖추도록 합시다. 특히 정기적으로 홈페이지, 웹사이트의 내용을 백업하고, 악의적인 공격자에 의해 홈페이지나 웹사이트의 내용이 위조, 변조되지는 않았는지 점검하고, 필요시 공격받지 않은 시점의 백업을 이용하여 복원하는 절차를 마련해야 합니다.

76 https://www.etnews.com/20150501000111

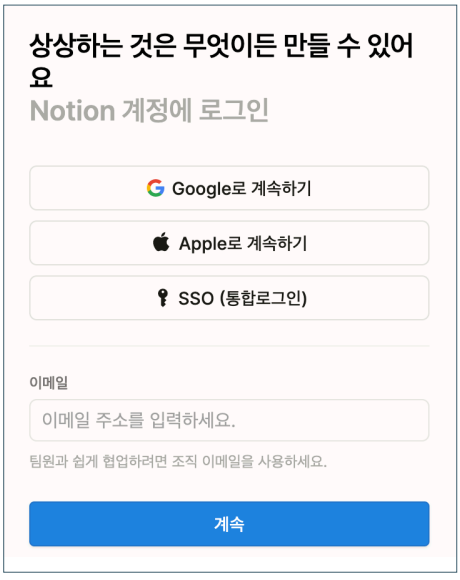
7. 클라우드 서비스 및 협업 툴 보안

7-1. 주요 클라우드 서비스 및 협업툴 사용시 주의점

7-1-1. 노션(Notion) 필수 설정

노션(Notion, https://notion.so)은 클라우드 기반의 콘텐츠 공유 협업 도구입니다. 좀더 안전한 노션 사용을 위해 다음 사항들을 점검하세요.

로그인 방식에 대한 검토



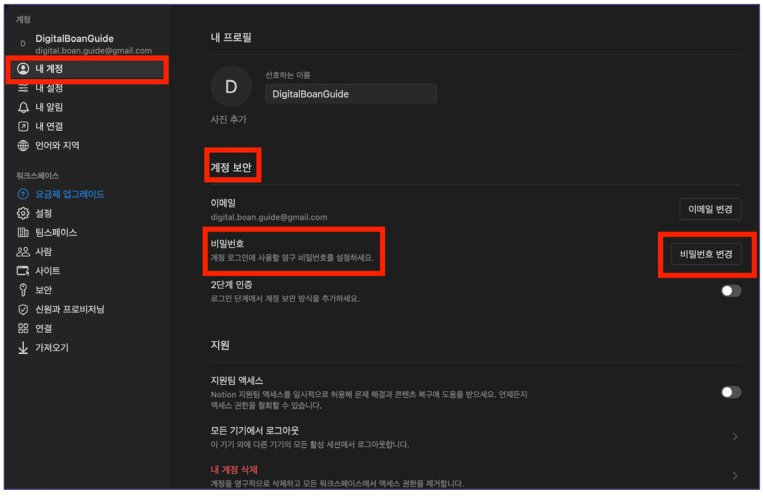
노션에 로그인하는 방법에는 여러 가지가 있지만, Google 계정이나 애플 계정을 사용하는 방법과 이메일 주소를 사용하는 방법이 있습니다. Google 계정이나 애플 계정을 사용한다면, 노션 계정의 보안 수준은

Google 계정이나 애플 계정의 보안 수준을 그대로 따라가게 됩니다. <디지털 보안 대책 마련하기> 및 <디지털 보안을 위한 7가지 원칙>에서 설명했듯이, Google 혹은 애플 계정의 디지털 보안이 취약하면 노션 디지털 보안도 마찬가지로 취약해진다는 점을 참고하세요.

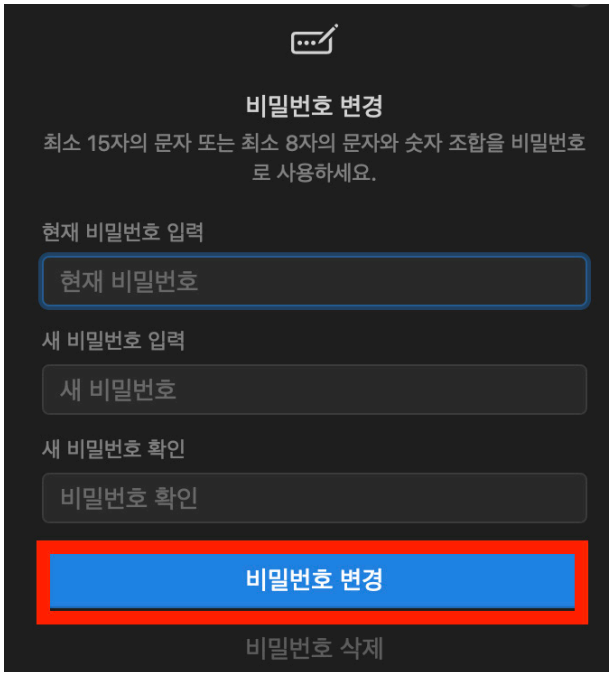
비밀번호를 사용하지 않도록 설정하기

이메일 주소로 노션에 로그인한다면, 두 가지 사항을 고려해야 합니다. 하나는 비밀번호를 사용하지 않도록 설정하는 방향입니다. 이렇게 하면 노션에 로그인할 때마다 노션에서 1회성 비밀번호(인증코드)가 담긴 이메일을 보냅니다. 노션 비밀번호가 유출되는 것에 대한 위협을 덜 수 있지만, 반대로 이메일 받은 편지함을 열어볼 수 있는 사람으로부터는 노션 계정을 보호할 수 없습니다.

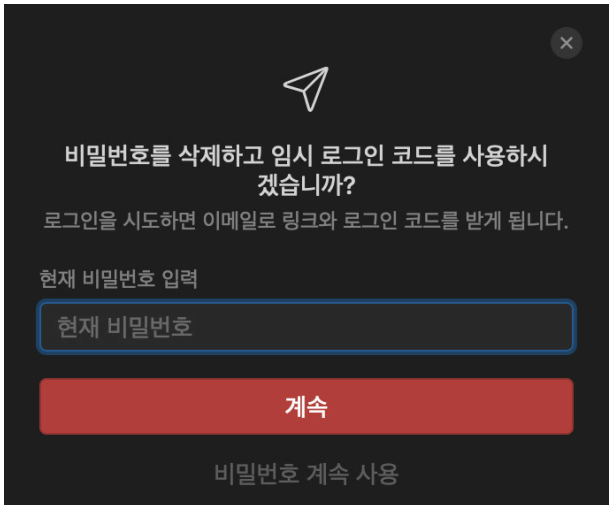
비밀번호를 삭제하는 방법을 소개합니다. 먼저 노션 화면 왼쪽의 [설정과 멤버] 탭에서 [내 계정] →[계정 보안] → [비밀번호] → [비밀번호 변경]을 클릭합니다.



이어서, [비밀번호 삭제]를 클릭합니다.



현재의 비밀번호를 입력하고 [계속]을 누릅니다.



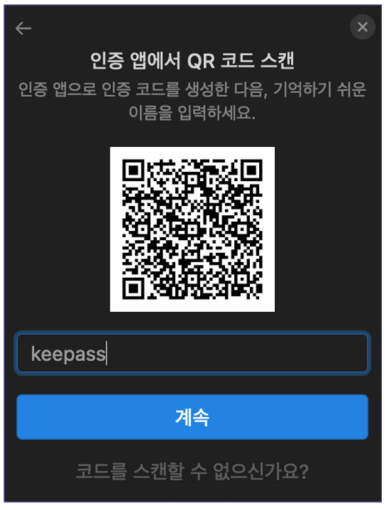
이후 노션에 로그인하려면, 이메일 주소를 입력하고, 이메일 주소로
“임시 Notion 코드는 <????-?????-?????-?????>입니다”라는
메일이 오면 이 코드를 사용하면 됩니다.

비밀번호와 함께 2단계 인증(2FA) 사용하기

클라우드 기반 협업 툴 노션의 필수 보안 설정 중 하나로
2단계 인증의 사례를 소개합니다.

비밀번호는 지식 기반 인증 방식입니다. 비밀번호를 모르는 사람은
들여보내지 않고, 비밀번호를 아는 사람은(지식을 가진 사람은) 들여보내는
방식입니다. 따라서 내 노션 계정의 비밀번호를 아는 사람은 설령 나
자신이나 우리 조직의 구성원이 아니더라도 노션에 로그인할 수 있게 됩니다.
이를 막기 위해 비밀번호 이외에 추가로 2단계 인증을 적용할 수 있습니다.

먼저 노션 화면 왼쪽의 [설정과 멤버] 탭에서 [내 계정] →
[계정 보안] → [비밀번호] → [2단계 인증] 을 클릭합니다.



이어서 [Authenticator 앱 사용]을
클릭합니다. 화면에 TOTP 앱에
사용할 수 있는 QR 코드가
표시됩니다. 이제 사용중인 TOTP
앱(예를 들어 KeePassDX)을
사용하여 화면에 표시된
QR 코드를 스캔합니다.

스캔이 완료되어 TOTP 앱에
노션 TOTP 설정이 저장되면,

이제 TOTP 앱에서 생성된 6자리 숫자를 입력합니다. 그러면 노션에서 2단계 인증 설정에 대한 '백업 코드'를 알려줍니다. '백업 코드'를 안전한 장소에 저장하고 TOTP 등록을 완료합니다.

이제 노션에 로그인하려면 이메일 주소와 비밀번호를 아는 것만으로는 불가능합니다. QR 코드를 스캔하여 성공적으로 6자리 숫자를 생성했던 TOTP 앱이 있어야만 합니다.

만일 하나의 노션 계정을 여러 사람이 공유한다면 2단계 인증 수단 또한 여러 사람이 공유해야 합니다. 2단계 인증 수단을 여러 사람이 안전하게 공유하는 건 쉽지 않은 일일 수 있습니다. 만일 하나의 노션 계정을 여러 사람이 공유하면서 동시에 2단계 인증을 사용해야만 한다면, 권장하지 않는 방법이지만 2단계 인증을 위한 TOTP 앱을 등록하는 날을 정하고, 그 날 하루에 계정을 공유하는 모든 사람이 모여서 각자의 기기의 TOTP 앱에 일제히 코드 등록을 하는 방법을 사용할 수 있습니다. 또한 어떠한 경우에도 TOTP 앱에 등록된 QR코드가 유출되었다면 TOTP를 비활성화해야 합니다.

노션에서는 TOTP 이외에도 휴대전화의 문자메시지를 받는 방식을 제공합니다. 이 방식은 TOTP 처럼 처음에는 다소 사용법이 어려운 프로그램을 사용하지 않아도 된다는 장점이 있지만, 동시에 노션 계정에 휴대전화 번호를 연결해야 하는 점, 결국은 문자메시지를 경유하기 때문에 통신사 등에는 노션 사용에 대한 이력이 남을 수밖에 없는 점 등의 단점도 존재합니다.

정기적인 권한 관리 일정 마련하기

여러 사람이 함께 사용하는 노션 워크스페이스의 경우 일정한 주기마다 정기적으로 각종 권한을 관리하는 것이 좋습니다.

다음과 같은 항목들을 중점적으로 점검하세요.

✓ 워크스페이스 멤버 / 게스트 / 그룹 명단 확인

- 퇴사, 탈퇴 등의 이유로 더 이상 워크스페이스에 접근할 필요가 없는, 혹은 접근해서는 안 되는 계정에게 워크스페이스 접근 권한이 있는지 확인합니다.
- 노션 무료버전이 아닌 경우, 각각의 계정에게 '관리자'가 아닌 다른 권한을 부여하는 것이 바람직합니다. '관리자' 권한이 있으면 실수로 외부에 공유하면 안 되는 페이지를 공유하는 등의 위협이 발생할 수 있습니다.

✓ 페이지 수준 권한 확인

- 모든 멤버가 노션 워크스페이스 내의 모든 페이지에 대해 같은 수준의 권한을 가질 필요는 없습니다. 모든 멤버가 '편집 가능' 권한을 가질 필요가 있는지 검토하고, 가능한 한 작은 수준의 권한을 부여합니다.
- 특히 조직 외부 사람이 볼 수 있도록 홈페이지 용도나 공지 용도로 활용되는 노션 페이지의 경우 조직 내부의 누구나 편집할 수 있는 상황은 바람직하지 않습니다. '읽기 전용'이나 '댓글 허용'같은 축소된 권한을 부여하도록 합니다.

✓ 게시된 사이트 목록 확인

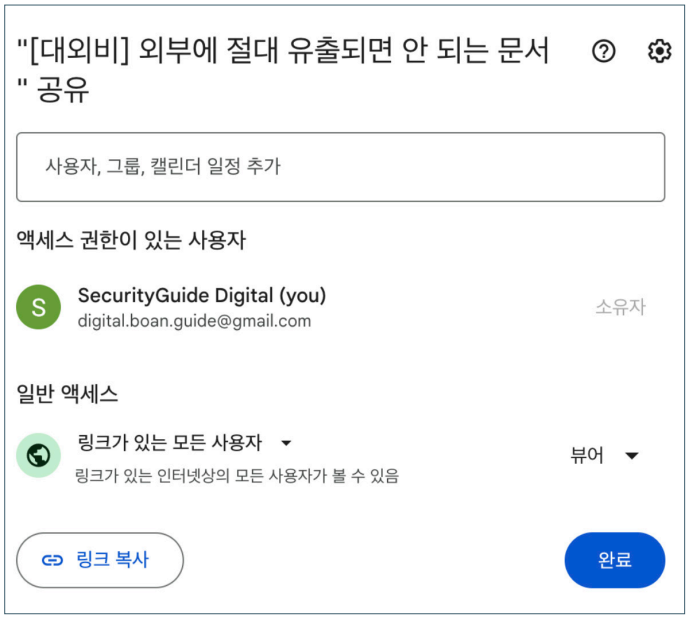
- 조직 외부 사람이 볼 수 있도록 공지할 목적으로 게시된 노션 페이지의 목록을 점검하고, 더 이상 게시되어 있을 필요가 없거나 게시되어서는 안 될 페이지가 게시되었다면 '게시 취소'를 진행합니다.
- 가능하면 조직 외부 사람이 볼 수 있도록 인터넷에 공유하는 페이지는 일정 기간 동안만 노출되도록 기간을 설정합니다.

7-1-2. 구글 드라이브(Google Drive) 필수 설정

구글 드라이브(Google Drive)는[77] 구글에서 제공하는 파일, 문서 공유 협업 클라우드 서비스입니다. 구글 독스(Google Docs)등을 아우르는 개념입니다. 좀더 안전한 구글 드라이브 사용을 위해 아래의 내용을 꼭 확인하세요.

꼭 필요하지 않다면 [링크가 있는 인터넷상의 모든 사용자가 볼 수 있음]으로 공유하지 않기

구글 문서를 사용하여 여러 사람, 조직에 회의록을 공유하는 경우가 많습니다. 아래 사진과 같이 [링크가 있는 모든 사용자]가 볼 수 있도록 설정하면 별다른 절차 없이 '링크' 주소만 있다면 문서의 내용을 자유롭게 열람할 수 있습니다.

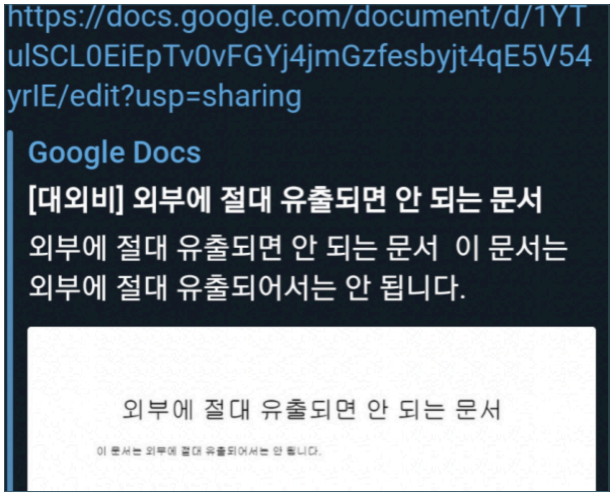


77 https://drive.google.com

문서의 '링크'를 메신저에 공유하면, 메신저의 종류에 따라 '링크'된 문서의 내용을 그림파일(썸네일)로 만들어 '미리보기'라는 형태로 서버에 저장하는 경우가 있습니다. 뒤늦게 문서의 권한을 변경하여도 메신저의 서버에는 문서의 내용이 그대로 남아있게 됩니다.

아무나 볼 수 없도록 공유 설정을 변경하면 위의 링크는 [액세스 권한 필요]라는 화면으로 연결됩니다.

하지만 위의 링크를 메신저에서 전달하면 메신저 대화창에는 해당 문서의 내용이 여전히 아래와 같이 '미리보기'가 남아있게 됩니다.



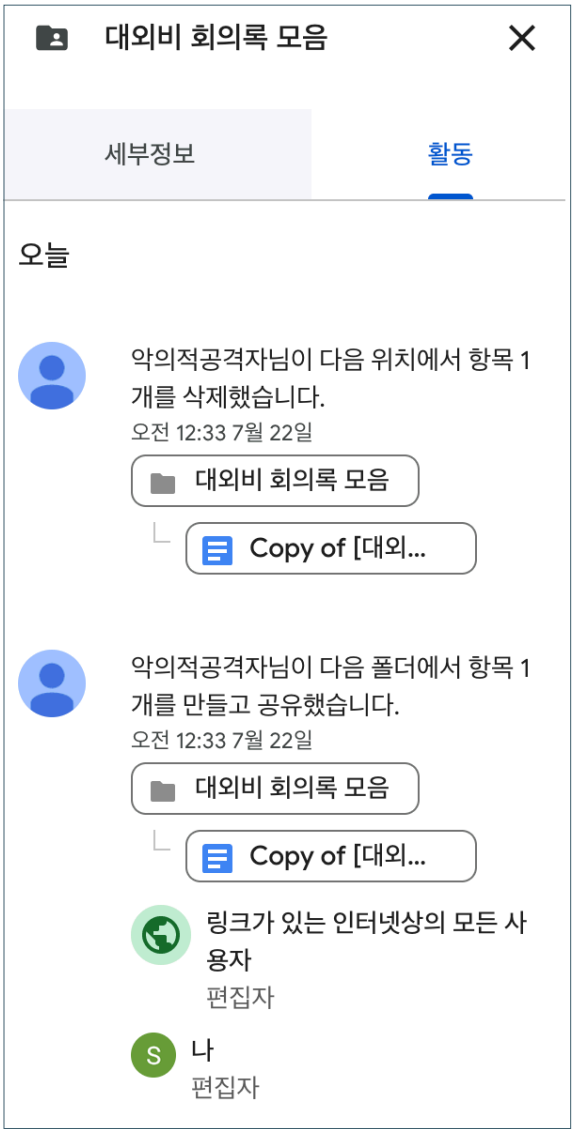
또한 과거 카카오톡에서는 카카오톡 대화창을 통해 누구나 열람할 수 있는 링크의 형태로 전달된 페이지를 다음 검색엔진에 노출하는 경우가 있었습니다.[78] 따라서 구글 드라이브를 통해 문서나 자료를 공유할 때에는 외부의 누구나 열람해도 되는 내용이 아니라면 [링크가 있는 모든 사용자]로 공유하지 말고, 반드시 열람할 수 있는 사람의 Google 계정 목록을 정하여 공유해야 합니다.

폴더 단위로 공유할 경우 폴더의 공유 권한 및 '활동' 로그 확인하기

구글 드라이브를 사용해 여러 개의 문서를 하나의 폴더로 묶어서 공유하는 경우가 많습니다. 이 때 폴더의 권한을 [링크가 있는 모든 사용자]에게 [편집 가능]으로 공유하였다면, 이 폴더를 통해 회의록 등이 유출되는 상황을 만날 수 있습니다.

78 https://m.dongascience.com/news.php?idx=12429

가급적 정해진 사람 이외에는 열람해서는 안 되는 문서는 [링크가 있는 모든 사용자]가 볼 수 있는 폴더에는 공유해서는 안 되며, 혹시라도 이러한 상황이 벌어졌는지 확인하기 위해서는 [활동] 탭을 주의깊게 살펴야 합니다.



7-1-3. 구글(Google) 계정의 '활성 세션' 검토

잠시 다른 사람의 컴퓨터를 빌려서 사용하는 등의 이유로 나 혹은 우리 단체의 Google 계정을 다른 사람의 기기에서 로그인해야 하는 경우가 있습니다. 이럴 때 실수로 로그아웃을 하지 않고 장소를 떠나거나 하는 실수는 치명적인 보안 사로고 이어집니다. [Google 계정] → [보안] → [모든 기기 관리] 메뉴를 사용하여, 현재 로그인이 유지되고 있는 '활성 세션'의 목록을 살펴보고 검토하세요. 필요하면 이 화면에서 특정 기기를 로그아웃시킬 수 있습니다.

7-2. 생성형 AI와 디지털 보안

7-2-1. 생성형 AI 사용으로 인한 보안 위협의 개요

마이크로소프트와 애플은 OS 자체에 생성형 AI가 탑재돼 있는 상황을 점점 더 만들어가고 있습니다. 아이폰을 사용하기만 하면 아이폰 사용자 스마트폰에 저장돼 있는 내용을 '시리'라고 하는 비서 앱이 챗GPT 등에 전송을 할 수 있게 해 주는 기능을 결합시키고 있습니다.

이러한 기능을 비활성화할 수 있는 선택지가 지속적으로 소비자들에게 주어질 수 있도록 하는 접근이 필요합니다. 개개인의 디지털 보안 대책에 따라 달리 선택할 수 있는 문제이기 때문입니다. 어떤 사람들에게는 생성형 AI를 운영하는 업체에게 이 파일이 전송되는 그 자체는 괜찮을 수 있습니다. 이런 사람들은 단지 업체가 생성형 AI로부터 파일이 유출되지 않게 보장해 주면 된다는 입장을 취할 수 있습니다. 혹은, 생성형 AI에게 파일이 전달되는 통제권을 확보하는 것 자체가 중요하다는 관점도 있을 수 있습니다. 운영체제에 내장되어 있는 생성형 AI가 내 파일들을 보지 못하도록 하는 옵션들이 계속해서 존재하도록 그런 빅테크 기업에게 요구할 수 있어야 합니다. 즉, 빅테크 기업들이 소비자가 생성형 AI를 쓰지 않으면 서비스를 못 쓰게 하는 상황을 용인하지 않는 움직임이 중요합니다.

또, 생성형 AI가 발전한다고 하더라도 생성형 AI가 스스로 우리 스마트폰 속에 있는 파일을 우리 허락 없이 가져갈 수 있는 상황은 단시일 내에 만들어지지 않을 겁니다. 그렇기 때문에 생성형 AI 서비스를 제공하는 기업은 나름대로 안전이 보장된다며 규제 완화를 추동할 것입니다. 이에 대해 의식적으로 생성형 AI에 대한 정보 제공을 거부하도록,

의도적으로 일일이 허용하지 않으면 기본적으로 생성형 AI에게 내 파일이 전달되지 않는 게 기본값이 되도록 계속해서 규제당국에 의견을 개진해야 합니다.

한편 생성형 AI의 학습 데이터 편향이 큰 이슈가 되는 지금, 어떻게 해야 인권 담론 등이 생성형 AI의 출력 결과물에 잘 반영되게 할 수 있는지도 중요한 주제입니다. 생성형 AI가 어떻게 해야 우리의 인권 담론 등을 조금 더 잘 이해하도록 훈련할 수 있는지, 혹시 생성형 AI 자체가 반인권적인 관념을 허용하는 방향으로 가고 있는 건 아닌지, 생성형 AI의 공급 업체가 그 업체의 직원들이 판단하는 윤리관에 입각하여 훈련되는지를 되짚어볼 필요가 있습니다.

생성형 AI 시대에 우리의 파일을 안전하게 관리할 수 있는 방법은 결국 다른 디지털 보안 대책과 크게 다르지 않습니다. 생성형 AI에게 우리 파일을 허락하지 않는 게 중요합니다. 생성형 AI가 파일을 허락 없이 가져갈 수 없는 상황이 유지되도록 규제하는 게 중요합니다. 또한 디지털 보안 가이드의 <1-1-1. 사례: 화상회의 참가자 모두가 딥페이크>에서 살펴본 것처럼 공격자는 생성형 AI를 사용하여 화상회의나 통화, 이메일, 메신저 등의 소통에서 좀더 정밀하게 타인을 사칭할 수 있습니다. 이러한 디지털 보안 침해 공격에 생성형 AI가 사용되지 않도록 생성형 AI 서비스를 제공하는 기업들이 안전장치를 마련할 것을 촉구하고, 동시에 규제되지 않는 생성형 AI 도구에 기반한 사칭 공격의 피해를 입지 않도록 소통에 주의를 기울여야 합니다.

8. 사무실, 물리적 보안 및 비대면 환경 보안

8-1. 물리적 보안의 중요성

디지털 보안의 중요한 요소 중 하나는 디지털 기기 자체에 대한 물리적인 보안입니다. 강력한 디지털 보안 수준의 메신저를 사용하더라도 그 메신저 앱의 화면을 근처에 있는 사람이 볼 수 있다면 아무런 소용이 없습니다. 따라서 정보가 표시되는 화면이나 기기 자체에 대한 보안 요소에 유의해야 합니다.

8-1-1. 사생활보호 필름 부착

사생활보호 필름(정보보호필름, 정보보안필름)을 사용하면 정면이 아닌 측면에서 내 기기의 화면에 표시된 정보를 보는 것을 막을 수 있습니다. 단, 사생활보호 필름을 부착하면 기기의 화면을 여러 사람이 함께 보면서 작업을 할 때 화면의 정면이 아닌 사선에 있는 사람에게는 화면의 내용이 보이지 않게 될 수 있습니다.

외부인이 방문할 수 있는 사무실에서 다른 사람과 함께 볼 필요가 없는 화면, 공공장소 등에서 오직 나 혼자 보는 화면에 표시되는 정보를 지키는 목적으로는 사생활보호 필름을 사용하는 것이 바람직합니다. 모니터, 노트북, 태블릿, 스마트폰 등 화면이 있는 기기에 부착할 수 있는 사생활보호 필름을 부착하거나 거치 형태로 사용하는 필름을 사용하는 방법도 있습니다.

8-1-2. 노출된 공간에서의 작업

카페나 도서관 등 야외, 공공장소 등에서 디지털 기기를 사용하여

작업을 할 때는 다양한 보안 위협에 노출될 수 있습니다.
시그널 등의 앱을 사용하여 종단간 암호화가 되는 전화통화를
하더라도 정작 통화를 하는 장소 자체에 다른 사람들이 있다면
통화의 내용을 근처에 있는 사람이 고스란히 엿들을 수 있습니다.

디지털 보안의 가장 약한 연결고리 중 하나가 물리적 보안이고,
이 중에서도 가장 취약한 부분이 노출된 공간에서 벌어지는 일입니다.
집회나 시위 장소에서 디지털 기기를 분실하거나 빼앗길 수도 있고,
디지털 기기를 사용하여 나누는 소통 내용을 가까이 있는
다른 사람들이 알아차리기 쉬울 수도 있습니다.

8-2. 네트워크 장비 보안

집이나 사무실에서 유선인터넷을 사용하는 경우, 이러한 유선인터넷을 한 대의 PC에만 연결하지 않고 여러 대의 PC와 연결하거나, 혹은 스마트폰이나 노트북 등을 무선으로 인터넷에 연결할 수 있도록 하는 이른바 '인터넷 공유기'를 사용하는 경우가 많습니다. 특히 사무실에서 사용하는 인터넷 공유기의 경우 사무실 안쪽의 컴퓨터들과 사무실 바깥의 인터넷을 연결해 주는 중요한 관문으로, 만일 인터넷 공유기가 해킹될 경우 사무실 안의 모든 기기에 심각한 디지털 보안 위협을 초래하게 됩니다. 인터넷 공유기를 통해 다양한 정보가 유출될 수 있기 때문입니다.[79]

인터넷 공유기를 사용중인 경우, 다음과 같은 항목들을 점검하세요.

8-2-1. 인터넷 공유기 관리자 비밀번호 설정

인터넷 공유기에 별도로 관리자 비밀번호를 설정하지 않았다면, 즉시 설정하세요. 잠시 사무실에 방문하여 인터넷 공유기에 연결하는 사람이 인터넷 공유기의 관리자 페이지에 접근하는 것을 막아야 합니다. 인터넷 공유기의 비밀번호 설정 방법은 각 공유기의 제조사의 설명서를 참고하세요. 흔히 관리자 계정이 admin 이고 비밀번호가 admin 으로 설정되어 있는 경우가 많습니다. 당연하지만 공격자들이 가장 먼저 시험해보는 조합이므로, 기본값의 설정을 방치하지 말고 적절하게 변경하세요.

다음은 한국에서 시장점유율이 높은 주요 인터넷 공유기 업체들의

79 https://news.kbs.co.kr/news/pc/view/view.do?ncd=7981836

인터넷 공유기 관리자 비밀번호 설정 가이드 링크입니다.

- 아이피타임(IPTime): https://iptime.com/iptime/?page_id=67&uid=26023&mod=document
- 에이수스(Asus): https://www.asus.com/kr/support/faq/1047761/
- 티피링크(TP-Link): https://www.tp-link.com/kr/support/faq/3316/

8-2-2. 인터넷 공유기 펌웨어 업데이트

PC, 스마트폰과 마찬가지로 인터넷 공유기 또한 보안 취약점이 발견되어 보안 업데이트가 이뤄지는 디지털 기기입니다.
PC, 스마트폰의 보안 업데이트를 하는 것처럼 인터넷 공유기 또한 보안 업데이트가 필요합니다. 인터넷 공유기와 같은 기기의 보안 업데이트는 '펌웨어'(Firmware) 업데이트라는 형태로 진행됩니다.
사용중인 인터넷 공유기 제조사의 설명서를 참고하여 인터넷 공유기의 펌웨어를 항상 최신 버전으로 업데이트하세요.

8-3. 비대면 환경 보안

코로나19 등의 영향으로, 일상이나 업무에서 여러 사람들이 같은 공간에 모이지 않은 채 비대면 화상회의 등의 형태로 업무를 진행하는 일이 점점 많아지고 있습니다. 하지만 앞서 소개했듯 화상회의, 음성통화 등에 생성형 AI, 딥페이크 기술 등을 사용하는 공격이 본격화되고 있는 추세입니다.

좀더 안전한 비대면 업무 환경을 위해 다음과 같은 사항을 고려하세요.

8-3-1. 화상회의 참석자의 신원 인증

화상회의에 참석한 사람이 참석대상자 본인이 맞는지, 혹시 제3의 인물이 사칭하고 있는 것은 아닌지 확인할 방법을 마련하세요. 화상회의 참석 시 특정한 비밀번호를 입력해야만 참석할 수 있도록 하면, 그러지 않는 것보다는 조금 더 안전하지만 비밀번호가 유출될 경우에 대응할 수 없습니다. 각 참석자가 사전에 약속된 계정을 사용하여 접속하였는지, 접속한 이후 적절한 방법으로 본인을 인증하게 할 수 있는지 확인하세요.

8-3-2. 화상회의 내용의 녹화, 녹취 가능성 고려

화상회의 플랫폼 차원에서 화상희의 내용을 녹화하거나 녹음하는 기능을 제공할 경우, 이렇게 녹화된 영상 혹은 녹음된 음성이 어떤 기기에 저장되는지 그 범위를 확인하세요.

설령 화상회의 플랫폼이 녹화 혹은 녹음 기능을 제공하지 않더라도, 화상회의 참석자들은 자신의 기기의 화면을 녹화하거나, 아니면 아예 별도의

녹음기 혹은 카메라를 이용하여 회의 내용을 보존할 수 있고, 사각지대를 이용할 경우 상대방이 이러한 행위를 하고 있는지의 여부를 알 수 없습니다.

종단간 암호화 등이 적용되는 화상회의 플랫폼을 사용하더라도 이러한 상황에 대해서까지 통제할 수는 없다는 점을 염두에 두어주세요.

9. 이미 벌어진 보안 사고 대처하기

보안 사고가 일어나지 않도록 예방하는 것도 중요하지만,
그만큼 중요한 것은 보안 사고가 일어났을 때 피해를
최소화할 수 있도록 빠르게 대처하는 것입니다.
추가적인 피해를 최소화하기 위해 보안 사고가
일어났는지를 알 수 있는 방법을 다양하게 마련하고,
각종 사고가 발생했을 때 대응할 방법들을 숙지합시다.

9-1. 기기 도난, 기기 분실 초동 대응

일상에서 가장 쉽게 일어날 수 있는 보안 사고는 스마트폰 등 디지털 보안 대책으로 지켜야 하는 기기를 물리적으로 잃는 것입니다. 기기를 도난당할 수도 있고 단순히 분실할 수도 있습니다. 어떤 형태로든 기기에 내가 접근할 수 없는 상황에서는 자신의 디지털 보안 대책에 따라 적절한 조치를 취해야 합니다. 기기의 위치를 확인하거나, 기기에서 접근할 수 있는 클라우드 계정을 비활성화하는 방법을 고려할 수 있습니다.

9-1-1. 기기 위치 찾기 및 원격으로 초기화하기

기기를 분실했을 때 시도할 수 있는 몇 가지 방법 중 하나는 기기의 위치를 찾는 것입니다. 만일 기기에서 위치 정보를 사용하도록 설정되어 있고 기기의 전원이 켜져 있다면 기기의 위치를 찾을 방법을 시도할 수 있습니다. 혹은 기기에 저장된 데이터를 원격으로 지우는 것도 고려할 수 있습니다.

안드로이드 기기 위치 찾기 및 초기화

내 스마트폰 등 분실한 안드로이드 기기에 로그인되어 있는 구글 계정으로 로그인하여, '내 기기 찾기' 페이지로 진입합니다. 기기가 켜져 있다면 기기의 위치를 여기서 대략적으로 확인할 수 있습니다.

기기의 데이터를 삭제하는 등의 작업을 구체적으로 진행하는 방법에 대해서는 안드로이드 고객센터의 [내 Android 기기 찾기] → [분실한 Android 기기 찾기, 잠그기 또는 초기화하기]에 설명된 내용을 따르면 스마트폰을 잠글 수 있습니다.

아이폰 기기 위치 찾기

내 스마트폰 등 분실한 아이폰 기기에 로그인되어 있는 아이클라우드 계정으로 로그인하여, '내 기기 찾기' 페이지로 진입합니다. 기기가 켜져 있다면 기기의 위치를 여기서 대략적으로 확인할 수 있습니다.

기기의 데이터를 삭제하는 등의 작업을 진행하려면 iOS의 '분실 모드'에 관한 설명을 참고하여 기기를 분실한 것으로 표시하고 데이터를 초기화할 수 있습니다.

윈도우 노트북 위치 찾기

내 노트북에 로그인되어 있는 마이크로소프트 계정으로 로그인하여, '내 장치 찾기' 페이지로 진입합니다. 기기가 켜져 있다면 기기의 위치를 여기서 대략적으로 확인할 수 있습니다.

삼성 스마트폰 위치 찾기

갤럭시 등 삼성 안드로이드 스마트폰을 사용하는 경우, 삼성 계정으로 로그인되어 있다면 'Samsung Find' 서비스를 사용해 기기 위치를 찾을 수 있습니다.

9-1-2. 분실한 기기의 '활성 세션' 종료하기

텔레그램 메신저 등의 클라우드 서비스에는 유출되면 곤란한 민감한 정보가 담겨있을 수 있습니다. 사용중인 개별 클라우드 서비스에서 분실한 기기로부터 연결되어 있는 '활성 세션'을 종료시켜 분실한 기기로부터의 예상치 못한 연결을 막읍시다. 디지털 보안 가이드의 <2-3-1. 주요 서비스들의 '활성 세션' 혹은 현재 로그인되어 있는 기기 목록 확인 방법>을 참고하여 활성 세션을 종료시킵니다.

9-1-3. 분실한 기기에 연결된 계정의 인증 방식 변경 혹은 비활성화

분실한 기기에 연결된 계정의 활성 세션을 비활성화하더라도 분실한 기기를 통해 계정의 인증 방식을 알아낼 여지가 있다면 단순히 활성 세션을 비활성화하는 것만으로는 충분하지 않습니다. 분실한 기기에 연결된 계정의 비밀번호를 변경하거나, 2단계 인증 수단을 해당 기기에서 다른 기기로 변경하는 등의 조치를 취하여 계정의 인증 가능성을 낮추세요.

분실한 기기에 연결된 계정의 인증 방식을 변경하는 것만으로 충분하지 않고 계정 자체를 비활성화하거나 삭제하는 것이 바람직한 경우도 있습니다. 만일 자신의 상황이 여기에 해당된다고 판단된다면 분실한 기기에 연결된 계정을 삭제하세요.

9-2. 인증 정보 유출 대응

아이디와 비밀번호만 알면 인증할 수 있는 서비스를 사용중인 경우,
내 아이디와 비밀번호가 유출되었음을 알게 되면 가능한 빠르게 비밀번호를
변경하여야 합니다. 비밀번호가 유출된 서비스뿐만 아니라 혹시라도
동일한 비밀번호를 사용중인 다른 계정이 있다면 이 또한 비밀번호를
변경해야 합니다. 만일 비밀번호 관리 도구를 사용중인데 비밀번호 관리
도구의 데이터베이스 파일과 마스터 비밀번호가 유출되었다면 비밀번호
관리 도구에서 사용중이던 모든 계정의 비밀번호를 변경해야 합니다.

비밀번호 유출 등 인증 정보가 유출되었는지의 여부를 빠르게
알아차릴 방법을 마련하고, 인증 정보 유출에 기민하게 대처하세요.

9-2-1. 비밀번호 유출 여부, 비정상적인 로그인 모니터링하기

내 아이디가 포함된 비밀번호 유출 DB가 등장했는지 정기적으로
확인하세요. 누군가가 내 계정으로 로그인했는지의 여부를 확인할
방법을 마련하세요. '새로운 환경 로그인 알림', '새로운 기기
로그인 알림'등 사용중인 서비스에서 제공하는 로그인 알림을
활성화하세요. 로그인 알림을 사칭하는 스미싱에 속지 않도록
로그인 알림이 어떤 형태로 제공되는지 평소에 익숙해지세요.

9-2-2. 비밀번호 변경하기

비밀번호를 변경할 때에는 이전에 사용한 적이 없는 새로운 비밀번호를
생성하여야 합니다. 비밀번호 관리 도구를 사용중이라면 비밀번호 관리

도구가 새로운 비밀번호를 생성하도록 하세요.
비밀번호 관리 도구의 마스터 비밀번호 등 본인이 직접 외워야 하는
비밀번호를 변경할 때는 <2-1-3. 강력한 비밀번호의 요건>을
숙지하여 적절한 비밀번호로 변경하세요.

부록1. 보안 위협 평가 체크리스트 (안)

가이드의 각 항목 중 어디를 먼저 읽어야 좋을지 판단을 돕기 위한 보안 위협 평가 체크리스트입니다. 체크리스트를 참고하여 각자의 상황에 맞는 새로운 체크리스트를 만드는 것이 좋지만, 우선 여기서부터 시작해 주세요. 체크리스트의 각 질문에서 '네', '아니오', '모릅니다' 중 어디에 해당되는지, 그리고 그것이 괜찮은지를 가이드 본문을 통해 확인합시다.

✓ 비밀번호와 인증

- 단체의 구성원 여러 사람이 동일한 계정을 사용하는 경우가 있나요?
- 단체의 구성원 여러 사람이 동일한 기계를 사용하는 경우가 있나요?
- 단체의 구성원에 변동(채용, 퇴사)이 있을 때 과거와 동일한 비밀번호를 사용하나요?
- 비밀번호를 외우기 어려워서 어딘가에 적어두는 구성원이 있나요?
- 단체의 계정에 누가 언제 접근했는지 추적할 수 있나요?
- 단체의 계정에 대한 해킹 시도가 있을 때 즉시 알람을 받고 있나요?
- 단체의 계정을 공공 장소나 외부의 기계에서 로그인하는 일이 있나요?
- 단체의 계정마다 할 수 있는 일의 범위가 역할에 맞게 제한되어 있나요?

✓ 파일, 기기, 운영체제 보안

- 단체 구성원의 기계가 분실되었을 때 취해야 하는 조치가 무엇인지 알고 있나요?
- 단체 사무실 컴퓨터의 디스크가 도난당하면 단체의 파일을 제3자가 열어볼 수 있나요?
- 단체에서 쓰는 기기들의 운영체제 보안 업데이트는 최신으로 유지하고 있나요?

✓ 물리적 보안

- 단체에서 사용중인 홈페이지에 악성코드가 삽입된 경우 이를 단체에서 알 수 있나요?
- 단체 사무실의 인터넷 공유기에 관리자 비밀번호가 설정되어 있나요?

✓ 통신, 이메일 및 메신저 보안

- 사용하고 있는 메신저는 종단간 암호화(E2EE)를 지원하고 있나요?
- 사용하고 있는 메일 서비스는 PGP 암호화를 지원하고 있나요?
- 어떤 웹사이트에 접속했는지를 제3자가 모를 수 있는 상황을 보장하기 위한 별도 조치가 이행되고 있나요?
- 어떤 웹페이지에서 무엇을 읽었는지 제3자가 모를 수 있도록 별도의 조치를 취하고 있나요?

부록2. 디지털 보안 참고자료

디지털 보안 가이드는 디지털 보안에 대한 이해를 높이기 위한 시작점입니다. 디지털 보안에 대한 다양한 내용을 찾아볼 수 있는 참고자료들을 소개합니다.

국내외 참고자료

2015 디지털 보안 가이드북

- 2015년 진보넷에서 발간된 보안 가이드북의 온라인 버전입니다.
- https://guide.jinbo.net/digital-security/guide-for-guide
- 2015년 진보넷에서 발간된 보안 가이드북의 책자 버전입니다.
- 201507_디지털보안 가이드북.pdf
- 2015 디지털 보안 가이드북의 참고자료 목록입니다.
- http://guide.jinbo.net/digital-security/references

슬로우뉴스 & 함께하는 시민행동: “다른 인터넷이 가능하다” 시리즈

- http://slownews.kr/13142

(영문) Electronic Frontier Foundation: Surveillance Self-Defense

- EFF에서 발간하고 계속 갱신하고 있는 디지털 보안 가이드입니다.
- https://ssd.eff.org/

(영문) Front Line Defenders, Security in-a-Box

- Tactical Technology Collective에서 시작하여 Front Line Defenders에서 유지보수하고 있는 디지털 보안 가이드입니다.
- https://securityinabox.org/en/

(영문) Front Line Defenders, Digital Protection

- Front Line Defenders 에서 운영하고 있는 디지털 보안 관련 자료 모음입니다.
- https://www.frontlinedefenders.org/en/programme/digital-protection

(영문) APC, Digital Security First Aid Kit for Human Rights Defenders

- APC 에서 운영하고 있는, 디지털 보안 사고 관련 자료입니다.
- https://www.apc.org/en/irhr/digital-security-first-aid-kit

(영문) Freedom of the Press Foundation

- Freedom of the Press 재단에서 운영하는 다양한
  온라인 디지털 보안 강의자료입니다.
- https://freedom.press/training/secure-communication/
- https://freedom.press/training/online-account-security/

(영문) ACCESS NOW: Encrypt all the things

- 모든 정보를 암호화하는 디지털 보안 대책 수립을 도와주는 캠페인 자료입니다.
- https://www.accessnow.org/encrypt-all-the-things/

(영문) Reset the net: Privacy Pack

- Reset the net에서 운영하는 개인정보 보안 관련 자료들입니다.
- https://pack.resetthenet.org

국내외 기관, 단체

한국인터넷진흥원(KISA) 보호나라

- https://www.boho.or.kr/

(영문) Let's Encrypt

- https://letsencrypt.org/


Digital
Security
Guide